TREND MICRO™

5.0 TREND MICRO™ Endpoint Encryption

Administratorhandbuch

Umfassende Endpunktverschlüsselung für gespeicherte Daten

Endpoint Security

Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und dem hierin beschriebenen Produkt ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung des Produkts die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der verfügbaren Dokumentation durch:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Trend Micro, das Trend Micro T-Ball-Logo, Control Manager, OfficeScan Endpoint Encryption, PolicyServer, Full Disk Encryption, File Encryption und KeyArmor sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2014. Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: APGM56401/140410

Release-Datum: Dezember 2014

Geschützt durch U.S. Patent-Nr.: Zum Patent angemeldet.

In dieser Dokumentation finden Sie eine Einführung in die Hauptfunktionen des Produkts und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung des Produkts aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen des Produkts sind möglicherweise in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base auf der Website von Trend Micro verfügbar.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp

Inhaltsverzeichnis

Vorwort

Vorwort ix

Dokumente x

Zielgruppe x

Dokumentationskonventionen xi

Info über Trend Micro xii

Teil I: Übersicht über Endpoint Encryption

Kapitel 1: Einführung in Endpoint Encryption

Info über Trend Micro Endpoint Encryption 1-2

Wichtigste Funktionen und Vorteile 1-2

Was ist neu in Version 5.0 Patch 1 1-4

Info über Verschlüsselung 1-9

Komponenten von Endpoint Encryption 1-10

Kapitel 2: Übersicht über Geräte und Benutzer

Endpoint Encryption - Geräte 2-2

Endpoint Encryption Benutzer 2-5

Authentifizierungsmethode 2-7

Teil II: Administration mit Trend Micro Control Manager

Kapitel 3: Erste Schritte mit Control Manager

Info über Integration des Control Managers 3-2

Control Manager Architektur 3-3

Zusammenfassung der Vorgänge zum Konfigurieren von Control Manager 3-7

PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen . 3-8

Verzeichnisverwaltung für PolicyServer konfigurieren 3-10

Eine Richtlinie erstellen 3-12

Kapitel 4: Dashboard, Widgets und Berichte

Das Dashboard verwenden 4-2

Grundlegendes zu Registerkarten 4-2

Grundlegendes zu Widgets 4-5

Endpoint Encryption Widgets verwenden 4-9

Kapitel 5: Richtlinien in Control Manager

Gruppen 5-2

Richtlinien verstehen 5-2

Grundlegendes zu Richtlinientypen 5-4

Grundlegendes zu Einstellungen für das Richtlinienziel 5-7

Grundlegendes zur Richtlinienliste 5-8

Grundlegendes zur Liste der verwalteten Server 5-31

Richtlinienvorlagen aktualisieren 5-36

Kapitel 6: Benutzer in Control Manager

Widget Endpoint Encryption Benutzer 6-3

Benutzer zu Endpoint Encryption hinzufügen 6-4

Benutzer suchen 6-10

Benutzer ändern 6-10

Arbeiten mit Kennwörtern 6-11

Mit Richtlinienmitgliedschaft arbeiten 6-17

Kapitel 7: Geräte in Control Manager

Gerät zu einer Richtlinie hinzufügen 7-3
Gerät aus einer Richtlinie entfernen 7-6
Widget Endpoint Encryption - Geräte 7-7
Ein Gerät suchen 7-9
Ein Software-Token abrufen 7-10
Wiederherstellungsschlüssel abrufen 7-11
Geräteattribute anzeigen 7-12
Gerät auslöschen 7-15
Gerät sperren 7-16
Ein Gerät zurücksetzen 7-17
Gerät aus dem Unternehmen löschen 7-17
Gelöschtes Gerät wiederherstellen 7-19

Teil III: Administration mit Endpoint Encryption PolicyServer MMC

Kapitel 8: Erste Schritte mit PolicyServer MMC

Info über PolicyServer MMC 8-2
Bei PolicyServer MMC anmelden 8-2
PolicyServer MMC-Benutzeroberfläche 8-4
Mit Gruppen und Benutzern arbeiten 8-6
Richtliniensteuerelemente verstehen 8-16
Agents deaktivieren 8-21

Kapitel 9: Richtlinien in PolicyServer MMC

Richtlinienübersicht 9-2
Automatische Synchronisierung von Richtlinien 9-15
PolicyServer Richtlinien 9-16
Richtlinien für Full Disk Encryption 9-21
File Encryption Richtlinien 9-28
Allgemeine Richtlinien 9-33

Kapitel 10: Gruppen in PolicyServer MMC

Info über Gruppen 10-2
Gruppenverwaltung 10-3
Offline-Gruppen 10-15

Kapitel 11: Benutzer in PolicyServer MMC

Benutzer zu Endpoint Encryption hinzufügen 11-3
Benutzer suchen 11-8
Benutzer ändern 11-9
Gruppenmitgliedschaft eines Benutzers anzeigen 11-10
Neuen Benutzer zu einer Gruppe hinzufügen 11-11
Vorhandenen Benutzer zu einer Gruppe hinzufügen 11-14
Standardgruppe eines Benutzers ändern 11-16
Benutzer das Installieren in eine Gruppe erlauben 11-17
Benutzer aus einer Gruppe entfernen 11-18
Alle Benutzer aus einer Gruppe entfernen 11-19
Gelöschtes Benutzer wiederherstellen 11-19
Arbeiten mit Kennwörtern 11-20

Kapitel 12: Geräte in PolicyServer MMC

Gerät zu einer Gruppe hinzufügen 12-3
Gerät aus einer Gruppe entfernen 12-4
Gerät aus dem Unternehmen löschen 12-5
Software-Token abrufen 12-6
Den Wiederherstellungsschlüssel verwenden 12-7
Geräteattribute anzeigen 12-8
Verzeichnisliste anzeigen 12-12
Gruppenmitgliedschaft anzeigen 12-12
Gerät auslöschen 12-13
Gerät sperren 12-14
Ein Gerät zurücksetzen 12-14
Gelöschtes Gerät wiederherstellen 12-15

Teil IV: Verwaltung von Endpoint Encryption Agents

Kapitel 13: File Encryption

Info über die File Encryption 13-2
File Encryption Authentifizierung 13-2
File Encryption Agent - Menü 13-11
File Encryption - Kontextmenü 13-15
File Encryption Archivverschlüsselung 13-16
File Encryption – Archivieren und brennen 13-21
File Encryption - Sicheres Löschen 13-22

Kapitel 14: Full Disk Encryption

Info über Full Disk Encryption 14-2

Endpoint Encryption Tools 14-2
Full Disk Encryption Preboot 14-3
Full Disk Encryption Konnektivität 14-19
Full Disk Encryption – Wiederherstellungskonsole 14-21
Full Disk Encryption Wiederherstellungsmethoden 14-34
Reparatur-CD 14-37
Patch-Verwaltung mit Full Disk Encryption 14-45

Kapitel 15: Encryption Management für Fremdprodukte

Info über Agents zur Encryption Management 15-2
Einschränkungen der Agent-Richtlinie der Encryption Management . 15-3
Encryption Management for Microsoft BitLocker 15-5
Encryption Management for Apple FileVault 15-11

Teil V: Erweiterte Verwaltung und technischer Support

Kapitel 16: Erweiterte Unternehmensfunktionen

Unternehmen - Wartung 16-2
Gelöschte Benutzer und Geräte wiederherstellen 16-11
Unternehmen - Protokollereignisse 16-12
Unternehmen - Berichte 16-17

Kapitel 17: Wartung und technischer Support

Wartungsvertrag 17-2
Ressourcen zur Fehlerbehebung 17-6
Kontaktaufnahme mit Trend Micro 17-8
Andere Ressourcen 17-9

Anhänge

Anhang A: Einführung in Trend Micro Control Manager

Control Manager Standard und Advanced A-3
Einführung in die Funktionen von Control Manager A-3
Control Manager Architektur A-5
Endpoint Encryption bei Control Manager registrieren A-8
Grundlegendes zum Benutzerzugriff A-9
Grundlegendes zum Produktverzeichnis A-17
Neue Komponenten herunterladen und verteilen A-41
Protokolle verwenden A-70
Grundlegendes zu Berichten A-74

Anhang B: PolicyServer Nachrichten-IDs

Anhang C: Endpoint Encryption Dienste

Anhang D: Richtlinienzuordnung zwischen Management-Konsolen

Anhang E: Integration von OfficeScan

Info über Trend Micro OfficeScan Integration E-2
Info über den Plug-in Manager E-3
OfficeScan installieren E-4
Plug-in-Programme verwenden E-5
Die OfficeScan Agent-Hierarchie E-5
Verteilung von Endpoint Encryption Agents E-10

Anhang F: Glossar

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Willkommen beim Administratorhandbuch für Trend Micro™ Endpoint Encryption™. In diesem Handbuch werden die Sicherheitsarchitektur, die Optionen der Management-Konsole, die Benutzerauthentifizierung und die Verwaltung von Endpunkten erläutert. In diesem Handbuch wird ebenfalls beschrieben, wie Sie die Management-Konsolen und Endpoint Encryption Agents konfigurieren, um die Sicherheitsziele zu unterstützen, wie Sie Endpoint Encryption Benutzer, Gruppen und Geräte bereitstellen, um Richtlinien zu implementierenm und wie Sie mit Hilfe von Berichten und Protokollen die Unternehmenssicherheit analysieren. Es enthält Informationen zu Konfigurationen zur Fehlerbehebung, die Arbeit mit Tools und die Lösung von Problemen.

Es werden folgende Themen behandelt:

- *Dokumente auf Seite x*
- *Zielgruppe auf Seite x*
- *Dokumentationskonventionen auf Seite xi*
- *Info über Trend Micro auf Seite xii*

Dokumente

In der Dokumentation zu Trend Micro Endpoint Encryption sind folgende Dokumente enthalten:

TABELLE 1. Produktdokumentation

DOKUMENT	BESCHREIBUNG
Administratorhandbuch	Enthält eine Beschreibung der Konzepte und Funktionen des Produkts sowie detaillierte Anweisungen zur Konfiguration und Verwaltung von PolicyServer, Full Disk Encryption und File Encryption.
Installations- und Migrationshandbuch	Enthält Erklärungen zu den Systemvoraussetzungen und detaillierte Anweisungen zur Verteilung, Installation, Migration und Aktualisierung von PolicyServer, Full Disk Encryption und File Encryption.
Online-Hilfe	Alle Produkte enthalten eine Möglichkeit zum Zugriff auf die Online-Hilfe. Die Online-Hilfe bietet Zugang zu kontextsensitiven HTML-Hilfethemen.
Readme-Datei	Enthält aktuelle Produktinformationen, die in der Online-Hilfe oder im Benutzerhandbuch noch nicht erwähnt sind. Zu den Themen gehören die Beschreibung neuer Funktionen, Lösungen bekannter Probleme und eine Liste bereits veröffentlichter Produktversionen.
Support-Portal	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält aktuelle Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Zielgruppe

Dieses Handbuch wurde für IT-Administratoren geschrieben, die Trend Micro Endpoint Encryption in mittleren bis großen Unternehmen einsetzen. Es richtet sich zudem an Helpdesk-Mitarbeiter, die Benutzer, Gruppen, Richtlinien und Geräte

verwalten. In dieser Dokumentation werden grundlegende Kenntnisse zu Geräten, Netzwerken und Sicherheit vorausgesetzt. Dazu gehören:

- Setup und Konfiguration der Endpunkt-Hardware
- Grundlegende Konzepte für die Endpunktverschlüsselung
- Partitionierung, Formatierung und Wartung der Festplatte
- Client-Server-Architektur

Dokumentationskonventionen

In der Dokumentation werden die folgenden Konventionen verwendet:

TABELLE 2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHREIBUNG	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Referenzen auf andere Dokumente
`Schreibmaschinenschrift`	Beispiele für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigationspfad >	Navigationspfad für den Zugriff auf ein bestimmtes Fenster Beispiel: **Datei** > **Speichern** bedeutet, auf der Benutzeroberfläche auf **Datei** und dann auf **Speichern** zu klicken
Hinweis	Konfigurationshinweise

KONVENTION	BESCHREIBUNG
Tipp	Empfehlungen oder Vorschläge
Wichtig	Informationen zu erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produkteinschränkungen
Warnung!	Kritische Aktionen und Konfigurationsoptionen

Info über Trend Micro

Trend Micro, weltweit führend in der Internet-Content-Security und der Bewältigung von Bedrohungen, hat sich als Ziel gesetzt, den globalen Austausch von digitalen Informationen für Unternehmen und Endverbraucher sicher zu machen. Mit einer Erfahrung von über 20 Jahren bietet Trend Micro Client-, Server- und Cloud-basierte Lösungen, die neue Bedrohungen schneller unterbinden und die Daten in physischen, virtuellen und Cloud-Umgebungen schützen.

Da neue Bedrohungen und Schwachstellen immer wieder auftauchen, bleibt Trend Micro seiner Verpflichtung treu, seine Kunden beim Sichern von Daten, Einhalten der Konformität, Senken der Kosten und Wahren der Geschäftsintegrität zu unterstützen. Weitere Informationen finden Sie unter:

http://www.trendmicro.com

Trend Micro und das Trend Micro T-Ball-Logo sind Marken von Trend Micro Incorporated und in einigen Rechtsgebieten eingetragen. Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der entsprechenden Unternehmen.

Teil I

Übersicht über Endpoint Encryption

Kapitel 1

Einführung in Endpoint Encryption

Dieses Kapitel besteht aus einer Einführung in die Funktionen und Merkmale von Endpoint Encryption.

Es werden folgende Themen behandelt:

- *Info über Trend Micro Endpoint Encryption auf Seite 1-2*
- *Wichtigste Funktionen und Vorteile auf Seite 1-2*
- *Was ist neu in Version 5.0 Patch 1 auf Seite 1-4*
- *Info über Verschlüsselung auf Seite 1-9*
- *Komponenten von Endpoint Encryption auf Seite 1-10*

Info über Trend Micro Endpoint Encryption

Trend Micro Endpoint Encryption ist ein Garant für den Datenschutz, indem auf Endpunkten gespeicherte Daten, Dateien und Ordner sowie Wechselmedien auf vielen verschiedenen Plattformen verschlüsselt werden. Endpoint Encryption bietet eine granuläre Steuerung von Richtlinien und lässt sich flexibel in andere Verwaltungstools von Trend Micro integrieren, einschließlich Control Manager und OfficeScan. Die innovativen Verteilungsfunktionen unterstützen Sie dabei, Agent-Software ohne großen Aufwand mit FIPS 140-2-konformer Hardware-basierter oder Software-basierter Verschlüsselung zu verteilen, die für Endbenutzer völlig transparent ist und die Produktivität nicht beeinträchtigt. Nach der Verteilung wird die Sicherheitsverwaltung für Endpunkte durch automatisierte Berichterstellung, Audits und Richtliniensynchronisierung mit Endpoint Encryption PolicyServer vereinfacht.

Endpoint Encryption unterstützt Funktionen, um Remote-Befehle zu verteilen, verlorene Daten wiederherzustellen und die Identität der Benutzer zu schützen, während die Richtliniensynchronisierung in Echtzeit beibehalten wird. Wenn ein Endpunkt verloren geht oder gestohlen wird, können Sie von einem entfernten Standort aus einen Befehl zum Zurücksetzen oder „Auslöschen“ geben, um unverzüglich die unternehmensinternen Informationen zu schützen. Es gibt ebenfalls viele Wiederherstellungstools, die Endbenutzer bei der Datenrettung in dem Fall unterstützen, dass die Festplatte beschädigt wird. Endpoint Encryption fügt sich nahtlos in die vorhandenen unternehmensinternen Kontrollfunktionen ein und unterstützt eine Vielzahl von Authentifizierungsmethoden, einschließlich der Integration in Active Directory und Ressourcen für Endbenutzer, die ihre Anmeldedaten vergessen haben.

Wichtigste Funktionen und Vorteile

In der folgenden Tabelle werden die Hauptfunktionen und Vorteile von Endpoint Encryption erklärt.

TABELLE 1-1. Wichtigste Funktionen in Endpoint Encryption

FUNKTION	VORTEILE
Verschlüsselung	• Schutz durch Full Disk Encryption, einschließlich MBR (Master Boot Record), Betriebssystem und alle Systemdateien • Hardware- und Software-basierte Verschlüsselung für gemischte Umgebungen • Umfassender Schutz von Dateien, Ordnern und Wechselmedien
Authentifizierung	• Flexible Authentifizierungsmethoden, einschließlich Einzel- und Multi-Faktor-Authentifizierung • Steuern der Kennwortstärke und Regelmäßigkeit von Kennwortänderungen • Richtlinienaktualisierungen vor der Authentifizierung und dem Systemstart • Konfigurierbare Aktionen für den Schwellenwert für die Eingabe falscher Kennwörter
Geräteverwaltung	• Richtlinien zum Schutz von Daten auf Endpunkten und Wechselmedien • Möglichkeit zum Sperren, Zurücksetzen, Löschen oder Auslöschen eines Geräts

FUNKTION	VORTEILE
Zentrale Verwaltung	• Flexible Verwendung entweder von PolicyServer MMC oder Control Manager zur Verwaltung von PolicyServer • Verteilung von Endpoint Encryption Agents auf Endpunkte, die bereits von OfficeScan verwaltet werden • Durchsetzung von Sicherheitsrichtlinien für Einzelpersonen oder Richtliniengruppen von einem einzigen Richtlinienserver aus • Unmittelbarer Schutz von Endbenutzerdaten durch Senden von Sperr- oder Löschbefehlen an verlorene oder gestohlene Endpoint Encryption Geräte • Automatisierte Durchsetzung von Richtlinien mit Korrekturen an Sicherheitsereignissen • Aktualisieren von Sicherheitsrichtlinien in Echtzeit vor der Authentifizierung, um Benutzer-Anmeldedaten vor dem Booten des Betriebssystems zu widerrufen
Aufzeichnung von Protokollen, Berichten und Auditing	• Erweiterte Berichtsfunktion und erweitertes Auditing in Echtzeit zur Einhaltung der Sicherheitsrichtlinien • Analysieren von Nutzungsstatistik mit geplanten Berichten und Warnmeldungen

Was ist neu in Version 5.0 Patch 1

Trend Micro Endpoint Encryption 5.0 Patch 1 umfasst viele neue Funktionen und Verbesserungen.

TABELLE 1-2. Was ist neu in Endpoint Encryption 5.0 Patch 1

NEUE FUNKTION	BESCHREIBUNG
Control Manager Lizenzverwaltung	Endpoint Encryption PolicyServer ist in die Lizenzverwaltung von Control Manager integriert. Control Manager unterstützt die folgenden Funktionen mit Endpoint Encryption: • Anzeigen der aktuellen Lizenzdaten von Endpoint Encryption • Verteilen einer Lizenz für eine Vollversion auf PolicyServer • Erneuern einer Lizenz in PolicyServer
Control Manager User-Centered Visibility	Endpoint Encryption ist in Control Manager User-Centered Visibility integriert. Die an Control Manager gesendeten Statusprotokolle enthalten Benutzerinformationen für die folgenden Endpoint Encryption Agents: • Full Disk Encryption • File Encryption • Encryption Management for Microsoft BitLocker • Encryption Management for Apple FileVault
Unterstützung für Netzwerkkarten und WLAN-Adapter	Endpoint Encryption unterstützt die folgenden Gruppen von Netzwerkkarten: • Intel Ethernet Controller I217 • Intel Ethernet Controller I218 Endpoint Encryption unterstützt ebenfalls den Intel Dual Band AC 7260 WLAN-Adapter.

TABELLE 1-3. Was ist neu in Endpoint Encryption 5.0

NEUE FUNKTION	BESCHREIBUNG
Neue Kommunikationsschnittstelle	In Endpoint Encryption 5.0 wurde eine neue Kommunikationsschnittstelle (Endpoint Encryption Dienst) eingeführt, über die alle Endpoint Encryption 5.0 Patch 1 Agents und Management-Konsolen mit PolicyServer kommunizieren. Der Endpoint Encryption Dienst verwendet eine Representational State Transfer Web-API (RESTful) mit einem AES-GCM-Verschlüsselungsalgorithmus. Der Endpoint Encryption Dienst hat drei Hauptfunktionen: • Zugriffssteuerung: Nach der Benutzerauthentifizierung generiert PolicyServer ein Token für den betreffenden Benutzer, das nur für diese Sitzung gültig ist. • Richtliniensteuerung: Vor der Benutzerauthentifizierung beschränkt der Endpoint Encryption Dienst alle Transaktionen von PolicyServer MMC, Control Manager und OfficeScan bis nach der Benutzerauthentifizierung. • Automatische Richtlinien-Updates: Nach der Registrierung bei PolicyServer rufen die Endpoint Encryption Agents automatisch neue Richtlinien ohne Benutzerauthentifizierung ab.
Integration des Control Managers	Endpoint Encryption 5.0 ist in Control Manager zur Verwaltung von PolicyServer integriert. Informationen zu Control Manager finden Sie unter *Info über Integration des Control Managers auf Seite 3-2*.
Integration von OfficeScan	Endpoint Encryption 5.0 unterstützt OfficeScan Installationen. Mit dem neuen Plug-in für das Endpoint Encryption Verteilungstool können Sie Endpoint Encryption Agents auf einen beliebigen Endpunkt verteilen, der momentan von OfficeScan verwaltet wird, oder vom betreffenden Endpunkt deinstallieren.

Neue Funktion	Beschreibung
Lizenzverwaltung	Endpoint Encryption 5.0 ist in das Trend Micro Lizenzierungsportal integriert. Wie bei früheren Produktversionen können Sie Endpoint Encryption 30 Tage lang kostenlos ausprobieren. Nach Ablauf der Testlizenz ist ein Aktivierungscode erforderlich. Weitere Informationen zur Lizenzierung finden Sie unter *Wartungsvertrag auf Seite 17-2*.
Support für Apple FileVault™ und Microsoft BitLocker™	Endpoint Encryption 5.0 erweitert den Funktionsbereich von Full Disk Encryption, indem eine Integration mit Verschlüsselungslösungen, die zum Host-Betriebssystem gehören, durch zwei neue Endpoint Encryption Agents möglich gemacht wird: • Encryption Management for Microsoft BitLocker • Encryption Management for Apple FileVault Beide Agents werden zentral von PolicyServer über Richtlinien verwaltet, die bestimmen, ob das Endpoint Encryption Gerät von einem Remote-Standort aus gelöscht oder ausgelöscht werden soll.
Namensänderung von FileArmor und Wechsel zum Common Framework	Endpoint Encryption 5.0 benennt den FileArmor Agent in File Encryption um. Diese Änderung entspricht der neuen Funktionalität von Endpoint Encryption Agent besser. File Encryption verfügt über die Vorteile von FileArmor 3.1.3, einschließlich einer verbesserten Unterstützung für Wechselmedien. File Encryption wurde ebenfalls besser an Full Disk Encryption angepasst und unterstützt die verbesserte Kennwort- und Richtlinienverwaltung.

Neue Funktion	Beschreibung
Verbesserungen bei Wartung, Protokollen und Berichten	Endpoint Encryption 5.0 zeichnet sich durch mehrere Verbesserungen in Bezug auf die Produktwartung, die Protokolle und die Berichte aus. • Verfahren zum endgültigen Löschen der Protokolldatenbank: Es ist nun möglich, die Protokolldatenbank auf Grundlage spezifischer Kriterien endgültig zu löschen. Weitere Informationen finden Sie unter *Protokoll endgültig löschen auf Seite 16-8*. • Inaktive Endpoint Encryption Benutzer und Geräte löschen: Um Geräte und Benutzer im Unternehmen zu bereinigen, ist es nun möglich, Geräte und Benutzer endgültig zu löschen, die seit einer bestimmten Zeit inaktiv sind. Weitere Informationen finden Sie unter *Inaktive Geräte löschen auf Seite 16-5*. • Unternehmensbericht zu inaktiven Benutzern: Im neuen Unternehmensbericht werden alle Endpoint Encryption Benutzer aufgeführt, die sich seit einer bestimmten Zeit nicht bei einem Endpoint Encryption Gerät angemeldet haben. Weitere Informationen finden Sie in der aktualisierten Liste der verfügbaren Standardberichte unter *Standardberichte auf Seite 16-19*. • Unternehmensbericht zu inaktiven Geräten: Im neuen Unternehmensbericht werden alle Endpoint Encryption Geräte aufgeführt, bei denen sich seit einer bestimmten Zeit kein Endpoint Encryption Benutzer mehr angemeldet hat. Weitere Informationen finden Sie in der aktualisierten Liste der verfügbaren Standardberichte unter *Standardberichte auf Seite 16-19*.

Neue Funktion	Beschreibung
Smartcard-Verbesserungen	Endpoint Encryption 5.0 unterstützt die folgenden Smartcard-Verbesserungen: • Verbesserte Verteilung von Endpoint Encryption Agents in Umgebungen, in denen Smartcards verwendet werden • Unterstützung für gemeinsame Smartcard-Kennwörter

Info über Verschlüsselung

Verschlüsselung bezeichnet den Vorgang, mit dem Daten unlesbar gemacht werden, wenn kein Zugriff auf den zur Verschlüsselung verwendeten Schlüssel besteht. Sie können die Verschlüsselung durch eine Software- oder Hardware-basierte Verschlüsselung (oder eine Kombination aus beidem) vornehmen, um Daten zu schützen, die sich lokal auf einer Endpunkt-Festplatte, auf einem Wechselmedium oder in bestimmten Dateien und Ordnern befinden und die in Netzwerken oder im Internet übertragen werden. Die Endpunktverschlüsselung ist das wichtigste Mittel, um die Datensicherheit zu gewährleisten und die Einhaltung gesetzlicher Vorschriften zum Datenschutz sicherzustellen.

Info über FIPS

Die *Federal Information Processing Standard (FIPS) Publication 140-2* ist ein Gerätesicherheitsstandard der US-amerikanischen Regierung, der die Sicherheitsstandards für Verschlüsselungsmodule vorgibt. In der folgenden Tabelle werden die vier Stufen der FIPS 140-2-Sicherheit erklärt:

Tabelle 1-4. FIPS 140-2-Sicherheitsstufen

Stufe	Beschreibung
1	Alle Verschlüsselungskomponenten müssen sich auf der Produktionsstufe befinden und dürfen keine Sicherheitslücken aufweisen.

Stufe	Beschreibung
2	Beinhaltet alle Anforderungen von Stufe 1 und fügt physischen Manipulationsbeweis und rollenbasierte Authentifizierung hinzu.
3	Beinhaltet alle Anforderungen von Stufe 2 und fügt physischen Manipulationswiderstand und identitätsbasierte Authentifizierung hinzu.
4	Beinhaltet alle Anforderungen von Stufe 3 und fügt weitere physische Sicherheitsanforderungen hinzu.

Komponenten von Endpoint Encryption

Endpoint Encryption besteht aus einem zentralen Verwaltungsserver (PolicyServer), der die Richtlinien- und Protokolldatenbanken, die Authentifizierung und alle Client-Server-Aktivitäten verwaltet. Sie können mehrere eindeutige Endpoint Encryption Agents verteilen, die jeweils spezifische Verschlüsselungsaufgaben ausführen. Alle Endpoint Encryption Agents kommunizieren über einen verschlüsselten Kanal.

Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

Endpoint Encryption und OfficeScan können integriert werden. Mit dem Plug-in für das Endpoint Encryption Verteilungstool können Sie die Software des Endpoint Encryption Agent auf beliebige verwaltete OfficeScan Endpunkte verteilen.

Hinweis

Informationen zu Verteilungsszenarien finden Sie unter *Übersicht über Verteilung und Upgrade* im *Endpoint Encryption Installations- und Migrationshandbuch*.

In der folgenden Darstellung werden die Komponenten und Kommunikationsprotokolle von Endpoint Encryption illustriert.

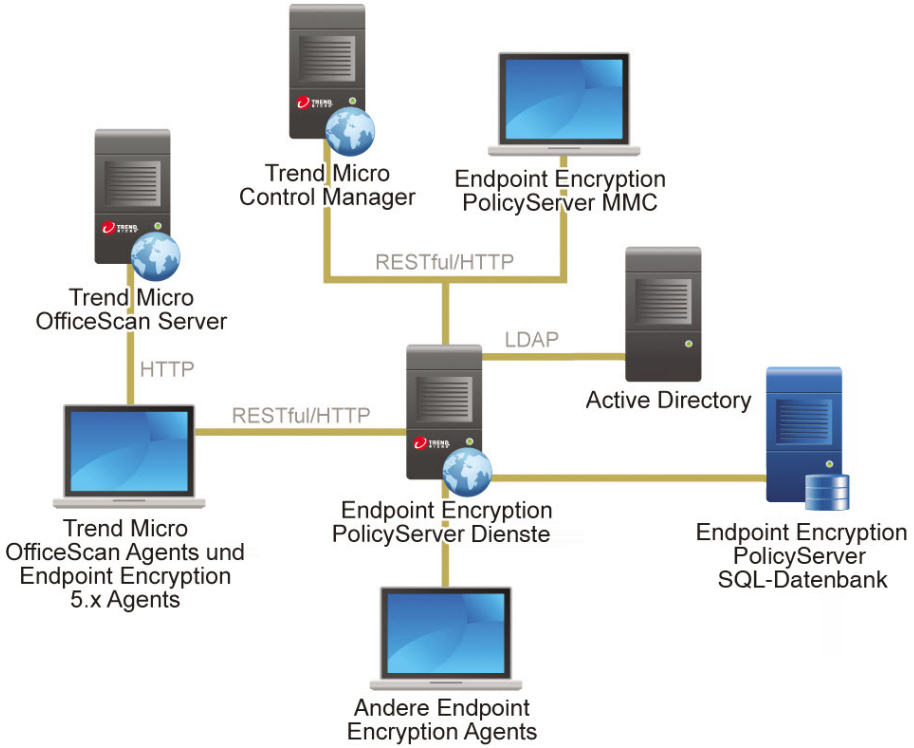


ABBILDUNG 1-1. Architektur von Endpoint Encryption

In der folgenden Tabelle werden diese Komponenten beschrieben.

TABELLE 1-5. Komponenten von Endpoint Encryption

KOMPONENTE	BESCHREIBUNG
Endpoint Encryption PolicyServer Dienste	PolicyServer besteht aus mehreren Diensten, die Richtlinien, Authentifizierung und Berichterstellung zentral steuern. PolicyServer besteht aus den folgenden Elementen: • Endpoint Encryption Dienst • Legacy Web-Service • PolicyServer Windows-Dienst Weitere Informationen zu PolicyServer finden Sie unter *Info über PolicyServer auf Seite 1-13*.
Endpoint Encryption PolicyServer SQL-Datenbank	In der Microsoft™ SQL Server-Datenbank werden alle Informationen zu Benutzern, Richtlinien und Protokollen gespeichert. Sie können die Datenbank auf demselben Server wie PolicyServer oder getrennt davon installieren. Sie können PolicyServer flexibel mit Microsoft SQL Server oder Microsoft SQL Express konfigurieren. Informationen zu den Optionen zur Datenbankkonfiguration finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.
Endpoint Encryption PolicyServer MMC	PolicyServer MMC ist die native Schnittstellenoption, um PolicyServer von einem Remote-Standort aus zu verwalten.
Trend Micro Control Manager	Trend Micro Control Manager ist eine Option, um PolicyServer von einem Remote-Standort aus zu verwalten, wobei die Lösung ebenfalls eine Integration mit anderen verwalteten Produkten von Trend Micro bereitstellt. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

KOMPONENTE	BESCHREIBUNG
Endpoint Encryption 5.0 Patch 1 agents	Alle Endpoint Encryption 5.0 Patch 1 Agents kommunizieren mit dem PolicyServer Endpoint Encryption Dienst unter Verwendung einer Web-API (RESTful). Weitere Informationen zu den Endpoint Encryption Agents finden Sie unter: • *Info über Full Disk Encryption auf Seite 14-2* • *Info über die File Encryption auf Seite 13-2* Informationen zur Kommunikation von Endpoint Encryption Agents finden Sie unter *Info über PolicyServer auf Seite 1-13*. **Hinweis** Sie können die Porteinstellungen während der Installation von Endpoint Encryption konfigurieren. Mit der Full Disk Encryption Wiederherstellungskonsole können Sie die zugewiesene Portnummer ändern.
Andere Endpoint Encryption Agents	Alle älteren Endpoint Encryption Agents (3.1.3 und älter) kommunizieren mit dem Legacy Web Service auf PolicyServer. Detaillierte Hinweise zur Kommunikation mit Agents finden Sie unter *Info über PolicyServer auf Seite 1-13*.
Active Directory	PolicyServer synchronisiert Benutzerkontoinformationen durch Kommunikation mit Active Directory über LDAP. Die Kontoinformationen werden in der Microsoft SQL-Datenbank zwischengespeichert. **Hinweis** Active Directory ist optional.

Info über PolicyServer

Trend Micro PolicyServer verwaltet Verschlüsselungsschlüssel und synchronisiert Richtlinien mit allen Endpunkten im Unternehmen. PolicyServer setzt ferner die sichere

Authentifizierung durch und umfasst Echtzeit-Audits und Tools zur Berichterstellung, um die Einhaltung von gesetzlichen Bestimmungen sicherzustellen. Sie können PolicyServer with PolicyServer MMC oder mit Trend Micro Control Manager flexibel verwalten. Andere Funktionen zur Datenverwaltung umfassen benutzerseitige Selbsthilfe-Optionen und Geräteaktionen, um ein verlorenes oder gestohlenes Gerät von einem entfernten Standort aus zurückzusetzen oder „auszulöschen“.

In der folgenden Tabelle werden die Komponenten von PolicyServer beschrieben, die Sie abhängig von den Anforderungen in der Umgebung auf einem oder mehreren Servern verteilen können.

TABELLE 1-6. Komponenten von PolicyServer

KOMPONENTE	BESCHREIBUNG
Unternehmen	"Endpoint Encryption - Unternehmen" ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. In einer PolicyServer Datenbank darf es nur eine Unternehmenskonfiguration geben.
Datenbank	In der Microsoft SQL-Datenbank von PolicyServer werden alle Benutzer, Geräte und Protokolldaten sicher gespeichert. Die Datenbank ist entweder auf einem dedizierten Server konfiguriert oder wird einem vorhandenen SQL-Cluster hinzugefügt. Die Protokoll- und anderen Datenbanken können sich an unterschiedlichen Speicherorten befinden.
PolicyServer Windows-Dienst	Der PolicyServer Windows-Dienst verwaltet alle Kommunikationstransaktionen zwischen Host-Betriebssystem, Endpoint Encryption Dienst, Legacy Web-Service, Client Web Proxy und SQL-Datenbanken.

Komponente	Beschreibung
Endpoint Encryption Dienst	Alle Endpoint Encryption 5.0 Patch 1 Agents nutzen den Endpoint Encryption Dienst zur Kommunikation mit PolicyServer. Der Endpoint Encryption Dienst verwendet eine Representational State Transfer Web-API (RESTful) mit einem AES-GCM-Verschlüsselungsalgorithmus. Nachdem sich ein Benutzer authentifiziert hat, generiert PolicyServer ein Token im Zusammenhang mit der spezifischen Richtlinienkonfiguration. Bis zur Authentifizierung durch den Endpoint Encryption Benutzer sperrt der Dienst alle Richtlinientransaktionen. Um eine dreistufige Netzwerktopographie zu erstellen, kann der Dienst auch gesondert auf einen Endpunkt verteilt werden, der sich in der Netzwerk-DMZ befindet. Dadurch kann sich PolicyServer sicher hinter der Firewall befinden. Informationen zu Verteilungsszenarien finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.
Legacy Web-Service	Alle Agents von Endpoint Encryption 3.1.3 und niedriger verwenden das Simple Object Access Protocol (SOAP), um mit PolicyServer zu kommunizieren. In bestimmten Situationen erlaubt SOAP möglicherweise unsichere Richtlinientransaktionen ohne Benutzerauthentifizierung. Legacy Web Service filtert SOAP-Aufrufe, indem eine Authentifizierung erforderlich gemacht wird und die Befehle begrenzt werden, die SOAP akzeptiert. Um eine dreistufige Netzwerktopographie zu erstellen, kann der Dienst auch gesondert auf einen Endpunkt verteilt werden, der sich in der Netzwerk-DMZ befindet. Dadurch kann sich PolicyServer sicher hinter der Firewall befinden. Informationen zu Verteilungsszenarien finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Management-Konsolen

Abhängig von den Anforderungen an die Endpunktsicherheit und die vorhandene Infrastruktur können Sie Endpoint Encryption nur mit einer Management-Konsole oder einer Kombination aus mehreren Management-Konsolen verwalten. In der folgenden Tabelle werden die verfügbaren Management-Konsolen zum Verwalten von Endpoint Encryption beschrieben.

TABELLE 1-7. Endpoint Encryption Management-Konsolen

MANAGEMENT-KONSOLE	BESCHREIBUNG
PolicyServer MMC	Das Plug-in PolicyServer Microsoft Management Console (PolicyServer MMC) ist die native Management-Konsole zur Verwaltung von Richtlinien, Benutzern und Geräten für Endpoint Encryption. Sie können mit PolicyServer MMC Folgendes zentral verwalten: • Alle Benutzer, Geräte und Gruppen von Endpoint Encryption • Alle Verschlüsselungs-, Kennwortkomplexitäts- und Authentifizierungsrichtlinien • Remote-Aktionen zur Gerätemanipulation, inkl. Auslöschen eines Geräts, Löschen von Daten oder Verzögern der Authentifizierung • Ereignisprotokolle über Authentifizierungsereignisse, Verwaltungsereignisse und Sicherheitsverstöße sowie den Geräteverschlüsselungsstatus • Remote-Hilfe zum Zurücksetzen des Kennworts • Optionen für Audits und Berichterstellung

MANAGEMENT-KONSOLE	BESCHREIBUNG
Control Manager	Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk. Sie können eine mehrschichtige Sicherheit schaffen, indem Sie Endpoint Encryption mit Control Manager als verwaltetes Trend Micro Produkt integrieren. Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.
OfficeScan	OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet. Mit dem OfficeScan Plug-in für das Endpoint Encryption Verteilungstool können Sie Endpoint Encryption Agents auf einen beliebigen Endpunkt verteilen, der momentan von OfficeScan verwaltet wird, oder vom betreffenden Endpunkt deinstallieren.

Endpoint Encryption Agents

In der folgenden Tabelle werden die Endpoint Encryption Agents beschrieben, die für eine Vielzahl von Umgebungen verfügbar sind.

AGENT	BESCHREIBUNG
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen. Weitere Informationen finden Sie unter *Info über die File Encryption auf Seite 13-2*.
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung. Sie können mit Full Disk Encryption Datendateien, Anwendungen, Registrierungseinstellungen, temporäre Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien auf allen Windows-Endpunkten sichern. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Systeme, bis der Benutzer validiert wird. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.

AGENT	BESCHREIBUNG
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.

Hinweis

Endpoint Encryption 5.0 verfügt über keine KeyArmor Geräte. Es werden jedoch ältere KeyArmor Geräte unterstützt.

Kapitel 2

Übersicht über Geräte und Benutzer

In diesem Kapitel wird beschrieben, wie mit Endpoint Encryption die Identität der Benutzer und der Zugriff auf Endpunkte geschützt wird. Durch die ordnungsgemäße Konfiguration von Endpoint Encryption Benutzern, Richtliniengruppen und Geräten wird sichergestellt, dass Daten für nicht autorisierte Benutzer verschlüsselt bleiben und das Risiko von Datenverlusten aufgrund versehentlicher Offenlegung oder beabsichtigter Sabotage vermieden werden kann.

Es werden folgende Themen behandelt:

- *Endpoint Encryption - Geräte auf Seite 2-2*
- *Endpoint Encryption Benutzer auf Seite 2-5*
- *Authentifizierungsmethode auf Seite 2-7*

Endpoint Encryption - Geräte

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die bei PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

Sie können Richtlinienregeln festlegen, die automatisch nach zu vielen fehlgeschlagenen Authentifizierungsversuchen oder, wenn der Endpoint Encryption Agent veraltete Richtlinien hat, ausgelöst werden. Folgende Richtlinienregeln sind verfügbar:

- Zeitverzögerung
- Remote-Authentifizierung erforderlich
- Gerät löschen

PolicyServer kann unverzüglich bei verlorenen und gestohlenen Endpunkten aktiv werden, indem eine Remote-Aktion auf dem betreffenden Endpoint Encryption Gerät ausgeführt wird. Die folgenden Remote-Aktionen sind verfügbar:

- Software-Token
- Wiederherstellungsschlüssel
- Gerät auslöschen
- Gerät sperren
- Warmstart

Richtlinienregeln für Endpoint Encryption Geräte

In der folgenden Tabelle werden die Regeln der Sicherheitsrichtlinie für verlorene oder gestohlene Endpoint Encryption Geräte beschrieben. Abhängig von den Richtlinieneinstellungen wird nach zu vielen aufeinanderfolgenden erfolglosen Authentifizierungsversuchen an den Endpoint Encryption Geräten der nächste Authentifizierungsversuch verzögert, das Endpoint Encryption Gerät wird gesperrt oder

alle Daten, die vom jeweiligen Endpoint Encryption Agent kontrolliert werden, werden gelöscht.

TABELLE 2-1. Optionen zur Gerätesicherheit

SICHERHEITSOPTION	BESCHREIBUNG
Zeitverzögerung	Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen sperrt PolicyServer vorübergehend das Endpoint Encryption Gerät und benachrichtigt den Endpoint Encryption Benutzer diesbezüglich. Während der Zeitverzögerung ist die Möglichkeit zur Authentifizierung oder Kennwortzurücksetzung deaktiviert. Die Dauer der Zeitverzögerung wird von der Richtlinie bestimmt. Nach Ablauf der Zeitverzögerung ist der Benutzer wieder berechtigt, sich zu authentifizieren. **Hinweis** Der Endpoint Encryption Benutzer kann die Selbsthilfe- oder Remote-Hilfe-Authentifizierung verwenden, wenn er nicht bis zum Ablauf der Zeitverzögerung warten will.
Remote-Authentifizierung erforderlich	Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen sperrt PolicyServer vorübergehend das Endpoint Encryption Gerät, bis sich der Endpoint Encryption Benutzer an den technischen Support zur Durchführung einer Remote-Hilfe-Authentifizierung wendet. **Hinweis** Weitere Informationen finden Sie unter *Remote-Hilfe auf Seite 2-12*.

SICHERHEITSOPTION	BESCHREIBUNG
Gerät wird gelöscht	Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen löscht PolicyServer alle Daten, die vom jeweiligen Endpoint Encryption Agent kontrolliert werden. Wenn beispielsweise ein Full Disk Encryption Gerät "gelöscht" wird, werden alle Daten vom Endpunkt gelöscht, während beim Löschen eines File Encryption Geräts alle Dateien und Ordner auf der lokalen Festplatte oder auf den Wechselmedien gelöscht werden, die vom File Encryption Agent geschützt werden. **Warnung!** Der Endpoint Encryption Benutzer kann die gelöschten Daten nicht wiederherstellen.

Remote-Aktionen des Endpoint Encryption Geräts

In der folgenden Tabelle werden die Remote-Aktionen beschrieben, die PolicyServer an das Endpoint Encryption Gerät senden kann.

TABELLE 2-2. Endpoint Encryption Gerätesicherheit

GERÄTEAKTION	BESCHREIBUNG
Software-Token	Wenn Sie ein „Software-Token“ erstellen, wird eine eindeutige Zeichenfolge erstellt, mit deren Hilfe Endpoint Encryption Geräte entsperrt werden können. Auf diese Weise können Sie die Remote-Hilfe für Endpoint Encryption Benutzer ausführen, um vergessene Kennwörter zurückzusetzen.
Wiederherstellungsschlüssel	Wenn Sie einen „Wiederherstellungsschlüssel“ generieren, können Benutzer eine Festplatte entschlüsseln, wenn der Benutzer das ursprüngliche Kennwort oder den ursprünglichen Schlüssel vergessen hat. Der Wiederherstellungsschlüssel ist nur für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker Agents verfügbar, weil diese keine der anderen verfügbaren Wiederherstellungsmethoden in Full Disk Encryption verwenden.

GERÄTEAKTION	BESCHREIBUNG
Gerät auslöschen	Die Ausführung eines „Auslöschen“-Befehls löscht alle Endpoint Encryption Gerätedaten. Welche Daten gelöscht werden, ist abhängig vom Geltungsbereich der Daten, der vom verbundenen Endpoint Encryption Agent verwaltet wird. Wenn Sie beispielsweise einen „Auslöschen“-Befehl auf ein Full Disk Encryption Gerät ausführen, werden alle Daten vom Endpunkt gelöscht. Führen Sie dagegen einen „Auslöschen“-Befehl auf ein File Encryption Gerät aus, werden alle Dateien und Ordner auf dem lokalen Datenträger und auf den Wechselmedien gelöscht, die vom File Encryption Agent geschützt werden. Der „Auslöschen“-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert.
Gerät sperren	Wenn Sie den Befehl „Sperren“ auf das Endpoint Encryption Gerät anwenden, wird der Endpoint Encryption Benutzerzugriff verhindert, bis eine erfolgreiche Authentifizierung für die Remote-Hilfe durchgeführt wurde. Beim Sperren eines Gerät wird der Endpunkt neu gestartet und in einen Status gezwungen, der Remote-Hilfe erfordert. Der Sperren-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert.
Warmstart	Wenn Sie einen „Warmstart“-Befehl geben, wird der Endpunkt neu gestartet. Der Befehl wird das nächste Mal ausgeführt, wenn der Agent mit PolicyServer kommuniziert.

Endpoint Encryption Benutzer

Bei Endpoint Encryption Benutzern handelt es sich um alle Benutzerkonten, die manuell zum PolicyServer hinzugefügt oder die mit Active Directory synchronisiert wurden.

Endpoint Encryption verfügt über mehrere Typen von Kontorollen und Authentifizierungsmethoden, die eine umfassende, auf Identität basierende Authentifizierung und Verwaltung möglich machen. Mit Control Manager oder PolicyServer MMC können Sie Benutzerkonten hinzufügen oder importieren, die Authentifizierung steuern, mit Active Directory eine Synchronisierung durchführen und die Mitgliedschaft in Richtliniengruppen bei Bedarf verwalten.

Endpoint Encryption Benutzerrollen

In der folgenden Tabelle werden die Endpoint Encryption Benutzerkontentypen beschrieben, die für die verschiedenen Rollen innerhalb des Unternehmens oder der Richtliniengruppe gedacht sind. Jede Rolle bestimmt die Berechtigungen, die gewährt werden, wenn der Benutzer auf die Endpoint Encryption Management-Konsolen und Geräte zugreift.

TABELLE 2-3. Endpoint Encryption Kontenrollen

ROLLE	BESCHREIBUNG
Unternehmensadministrator	Gedacht für Administratoren, die Aufgaben auf Unternehmensebene ausführen, Diese Administratoren verfügen über administrative Rechte für alle Gruppen, Benutzer, Geräte und Richtlinien, unabhängig davon, wo sie sich innerhalb des Unternehmens befinden.
Gruppen- oder Richtlinienadministrator*	Gedacht für Administratoren, die Aufgaben in Bezug auf Gruppen oder Richtlinien ausführen. **Hinweis** Diese Berechtigungen gelten nicht für übergeordnete Gruppen, Gruppen auf derselben Hierarchieebene oder deren Untergruppen.
Unternehmensauthentifizierer	Gedacht für Helpdesk-Mitarbeiter, die Remote-Unterstützung für Benutzer anbieten, die ihr Endpoint Encryption Kennwort vergessen oder technische Probleme haben. Unternehmensauthentifizierer haben Berechtigungen, die für das Unternehmen konfiguriert werden können.
Gruppen- oder Richtlinienauthentifizierer*	Gedacht für Helpdesk-Mitarbeiter mit denselben Berechtigungen wie der Unternehmensauthentifizierer, mit der Ausnahme, dass diese Berechtigungen nur für die zugewiesene Gruppe oder Richtlinie gelten.
Benutzer	Gedacht für einfache Endbenutzer ohne spezielle Berechtigungen. Die Benutzerrolle kann sich nicht an Endpoint Encryption Management-Konsolen anmelden.

Hinweis

*Wegen der unterschiedlichen Richtlinienarchitektur führt Control Manager die Richtlinien- und Gruppenstruktur von PolicyServer MMC zusammen. Die folgenden Rollen sind in PolicyServer MMC und Control Manager identisch:

- Gruppenadministrator (PolicyServer MMC) und Richtlinienadministrator (Control Manager)
- Gruppenauthentifizierer (PolicyServer MMC) und Richtlinienauthentifizierer (Control Manager)

Authentifizierungsmethode

Für Endpoint Encryption Administratoren und Benutzer stehen mehrere Authentifizierungsmethoden zur Anmeldung an den Endpoint Encryption Geräten zur Verfügung. Die verfügbaren Methoden werden vom PolicyServer Richtlinienkonfiguration bestimmt.

TABELLE 2-4. Unterstützte Authentifizierungsmethoden

AUTHENTIFIZIERUNGS METHODE	BESCHREIBUNG
ColorCode™	Eine eindeutige Farbfolge.
Domänenauthentifizierung	Active Directory LDAP-Synchronisierung für Single Sign-On (SSO).
Festes Kennwort	Eine Zeichenfolge aus Zeichen, Ziffern und Symbolen.
PIN	Eine herkömmliche PIN.
Remote-Hilfe	Interaktive Authentifizierung für Benutzer, die ihre Anmeldedaten vergessen haben, oder für Geräte, deren Richtlinien nicht innerhalb eines bestimmten Zeitraums synchronisiert wurden.
Selbsthilfe	Kombinationen aus Fragen und Antworten, mit denen ein Benutzer ein vergessenes Kennwort zurücksetzen kann, ohne sich an den technischen Support zu wenden.

AUTHENTIFIZIERUNGS METHODE	BESCHREIBUNG
Smartcard	Eine physische Karte wird in Verbindung mit einer PIN oder einem festen Kennwort verwendet.

Wichtiger Hinweis zu den Anforderungen für PolicyServer MMC

Sie müssen die für die Endpoint Encryption Benutzer verfügbaren Authentifizierungsmethoden mit PolicyServer MMC konfigurieren. Es ist nicht möglich, mit Control Manager die zulässigen Authentifizierungsmethoden zu konfigurieren. Sie können jedoch Control Manager für die Domänenauthentifizierung konfigurieren.

Konfigurieren Sie in PolicyServer MMC Richtlinien für jeden Endpoint Encryption Agent.

- Informationen zu Full Disk Encryption finden Sie unter *Kennwortrichtlinien auf Seite 9-27*.
- Informationen zu File Encryption finden Sie unter *Anmelderichtlinien auf Seite 9-31*.

Hinweis

Die Remote-Hilfe-Authentifizierung wird durch die Richtlinienregeln des Endpoint Encryption Geräts ausgelöst. Die Richtlinienregeln für die Remote-Hilfe können sowohl mit PolicyServer MMC als auch mit Control Manager konfiguriert werden. Weitere Informationen finden Sie unter *Richtlinienregeln für die Remote-Hilfe auf Seite 2-12*.

Weitere Informationen zur Konfiguration der Domänenauthentifizierung finden Sie unter *Regeln der Domänenauthentifizierungsrichtlinie auf Seite 2-11*.

Einschränkungen bei der Authentifizierung

In der folgenden Tabelle werden die verfügbaren Authentifizierungsoptionen in PolicyServer MMC und in den Endpoint Encryption Agents beschrieben.

TABELLE 2-5. Einschränkungen bei der Authentifizierung

AGENT	AUTHENTIFIZIERUNGSOPTION					
	FESTES KENNWORT	DOMÄNENKENNWORT	SMART CARD	PIN	RSA	COLORCODE
PolicyServer MMC	●	●	●			
Control Manager	●	●				
OfficeScan	●	●				
Full Disk Encryption	●	●	●	●		●
File Encryption	●	●	●	●		●
KeyArmor	●		●	●	●	●

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

ColorCode

ColorCode™ ist eine einzigartige Authentifizierungsmethode, bei deren Entwicklung eine schnelle Eingabe und eine leichte Merkfähigkeit im Vordergrund standen. Die ColorCode-Authentifizierung besteht nicht aus alphanumerischen Zeichen oder

Symbolen, sondern aus einer vom Benutzer erstellten Farbfolge (Beispiel: rot, rot, blau, gelb, blau, grün).

ABBILDUNG 2-1. Das Fenster "ColorCode-Authentifizierung"

Domänenauthentifizierung

Endpoint Encryption kann in Active Directory mit LDAP integriert werden, das in PolicyServer konfiguriert wird. Die Domänenauthentifizierung von Endpoint Encryption ermöglicht es Benutzern von Endpoint Encryption, SSO (Single Sign-On) zwischen dem Betriebssystem und dem Endpoint Encryption Agent einzusetzen. Benutzer von Endpoint Encryption mit Domänenauthentifizierung müssen nur einmal ihre Anmeldedaten für die Authentifizierung für Full Disk Encryption Preboot, Anmeldung bei Windows und den Zugriff auf die Dateien, die durch File Encryption geschützt werden, eingeben.

Vergewissern Sie sich, ob die folgenden Voraussetzungen erfüllt sind, damit die Active Directory-Integration nahtlos bewerkstelligt werden kann:

- Alle Endpoint Encryption Geräte befinden sich in derselben Domäne wie PolicyServer.
- Der in Active Directory konfigurierte Benutzername stimmt genau mit dem Benutzernamen überein, der in PolicyServer (einschließlich Groß- oder Kleinschreibung) konfiguriert wurde.
- Der Benutzername befindet sich innerhalb einer PolicyServer Gruppe und die Richtlinie "Domänenauthentifizierung" ist aktiviert.
- Der Host-Name und der Domänenname sind auf Grundlage von LDAP oder den Servereinstellungen für Active Directory ordnungsgemäß konfiguriert.

Hinweis

Informationen zur Konfiguration von Einstellungen für LDAP und Active Directory finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*, das Sie unter folgender Adresse finden:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Regeln der Domänenauthentifizierungsrichtlinie

Sie können die Domänenauthentifizierung mit Hilfe einer der folgenden Methoden aktivieren:

- Bearbeiten oder ändern Sie in Control Manager die **Benutzer**-Regeln einer Richtlinie.

  Weitere Informationen finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

- Navigieren Sie in PolicyServer MMC zu **[Gruppenname]** > **Richtlinien** > **Allgemein** > **Authentifizierung** > **Netzwerkanmeldung** > **Domänenauthentifizierung**.

Hinweis

Informationen zur Konfiguration von Einstellungen für LDAP und Active Directory finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*, das Sie unter folgender Adresse finden:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Festes Kennwort

Die Authentifizierung mit festem Kennwort ist die gängigste Authentifizierungsmethode. Das feste Kennwort wird vom Benutzer angelegt. Dabei kann es sich fast um jede Zeichenfolge aus Ziffern, Buchstaben und Symbolen handeln. Sie können für feste Kennwörter Einschränkungen festlegen, um sicherzustellen, dass diese nicht leicht missbraucht werden können.

PIN

Eine PIN ist die gängigste Identifizierungsmethode, bei der die Eingabe einer eindeutigen Zahlenfolge erforderlich ist. Die PIN wird vom Benutzer angelegt und kann fast alles sein. Wie bei festen Kennwörtern können Sie auch für PIN-Kombinationen Einschränkungen festlegen.

Remote-Hilfe

Mit der Remote-Hilfe können Gruppen- oder Unternehmensauthentifizierer ausgesperrte Endpoint Encryption Benutzer unterstützen, die sich nach zu vielen erfolglosen Versuchen oder, wenn zu viel Zeit seit der letzten PolicyServer Synchronisierung vergangen ist, nicht bei Endpoint Encryption Geräten anmelden können.

Richtlinienregeln für die Remote-Hilfe

In der folgenden Tabelle werden die Speicherorte der Richtlinien für die Konten- und Gerätesperrung beschrieben, die sich auf die Remote-Hilfe-Authentifizierung auswirken.

Diese Informationen vermitteln ein Verständnis dafür, welche Richtlinien festgelegt werden sollten.

TABELLE 2-6. Richtlinienspeicherorte für die Remote-Hilfe

NAME DER RICHTLINIE	MENÜPFAD FÜR POLICYSERVER MMC	MENÜPFAD FÜR CONTROL MANAGER	BESCHREIBUNG
Kontosperraktion	**Anmelden** > **Kontosperraktion**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Kontosperraktion**	Die Maßnahme, die durchgeführt wird, nachdem die Zeitdauer in „Kontosperraktionen “ abgelaufen ist. Mögliche Maßnahmen sind: Löschen, Remote-Authentifizierung
Zeitraum bis Kontosperrung	**Anmelden** > **Zeitraum bis Kontosperrung**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Konto sperren nach [ ] Tagen**	Die Anzahl von Tagen, die ein Gerät ohne Kommunikation mit PolicyServer sein kann, bevor die „Kontosperraktion“ ausgeführt wird.
Aktion zur Gerätesperrung	Für jeden Agent: **Anmelden** > **Aktion zur Gerätesperrung**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Aktion zur Gerätesperrung**	Die Aktion, die durchgeführt wird, wenn der in der Richtlinie „Zulässige Anzahl fehlgeschlagener Anmeldeversuche“ festgelegte Wert überschritten wurde. Unterstütze Maßnahmen: Zeitverzögerung, Löschen, Remote-Authentifizierung

Name der Richtlinie	Menüpfad für PolicyServer MMC	Menüpfad für Control Manager	Beschreibung
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Für jeden Agent: **Anmelden** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche, bevor die Aktion zur „Gerätesperrung“ ausgeführt wird.

Selbsthilfe

Mit der Selbsthilfe-Authentifizierung können Endpoint Encryption Benutzer, die ihre Anmeldedaten vergessen haben, ohne die Hilfe durch den technischen Support Sicherheitsfragen beantworten und sich bei Endpoint Encryption Geräten anmelden. Die Selbsthilfe ist für Unternehmens- oder Gruppenadministrator- und Authentifiziererkonten nicht verfügbar. Die Selbsthilfe macht es erforderlich, dass Endpoint Encryption Benutzer auf die persönlichen Fragen der Selbsthilfe mit ihren vordefinierten persönlichen Antworten reagieren. Mit der Selbsthilfe kann ein festes Kennwort oder eine andere Authentifizierungsmethode ersetzt werden.

Hinweis

Die Selbsthilfe kann nur mit PolicyServer MMC konfiguriert werden.

Vergewissern Sie sich, dass die Selbsthilfe-Authentifizierung zugelassen wird. Weitere Informationen finden Sie unter *Authentifizierungsrichtlinien auf Seite 9-34*.

Warnung!

Die Selbsthilfe kann aus maximal sechs Fragen bestehen. Erstellen Sie nicht mehr als sechs Fragen, sonst können sich die Benutzer nicht mit der Selbsthilfe-Authentifizierung anmelden.

SmartCard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch ein physisches Token zur Bestätigung der Identität des Benutzers. Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- Das Smartcard-Lesegerät ist mit dem Endpunkt verbunden, wobei sich die Smartcard im Lesegerät befindet.
- ActivClient 6.1 ist mit alle Service Packs und Updates installiert.
- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.

Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Hinweis

Smartcard-Authentifizierung kann nur mit PolicyServer MMC konfiguriert werden.

Aktivieren Sie die Smartcard-Authentifizierung für jeden Endpoint Encryption Agent:

- Navigieren Sie für File Encryption zu **Anmelden** > **Kennwort** > **Physischer Token erforderlich**.
- Navigieren Sie für Full Disk Encryption zu **Full Disk Encryption** > **Anmelden** > **Token-Authentifizierung**.

Smartcard-Registrierung

Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Registrieren Sie eine Smartcard, indem Sie eine der folgenden Methoden anwenden:

- Informationen zur Verwendung von Full Disk Encryption Preboot finden Sie unter *Eine Smartcard in Full Disk Encryption Preboot registrieren auf Seite 11-27*.
- Informationen zur Verwendung von PolicyServer MMC finden Sie unter *Smartcard-Authentifizierung in PolicyServer MMC konfigurieren auf Seite 11-25*.

Teil II

Administration mit Trend Micro Control Manager

Kapitel 3

Erste Schritte mit Control Manager

In diesem Kapitel werden die ersten Schritte mit Trend Micro Control Manager zur Verwaltung von PolicyServer beschrieben.

Es werden folgende Themen behandelt:

- *Info über Integration des Control Managers auf Seite 3-2*
- *Control Manager Architektur auf Seite 3-3*
- *Zusammenfassung der Vorgänge zum Konfigurieren von Control Manager auf Seite 3-7*
- *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 3-8*
- *Verzeichnisverwaltung für PolicyServer konfigurieren auf Seite 3-10*
- *Eine Richtlinie erstellen auf Seite 3-12*

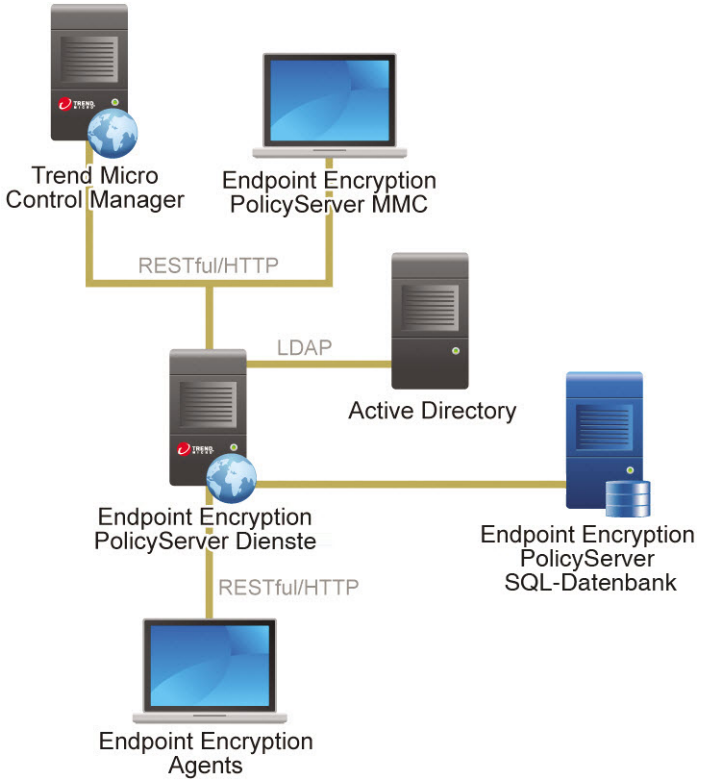
Info über Integration des Control Managers

Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

Mit Control Manager kann der Systemadministrator Aktivitäten wie beispielsweise auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Viren-/Malware-Eintrittsstellen überwachen und aufzeichnen. Der Systemadministrator kann Update-Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Zu den Beispielen für Update-Komponenten zählen die Viren-Pattern-Dateien, die Scan Engine und die Anti-Spam-Regeln. Mit Control Manager sind sowohl manuelle als auch zeitgesteuerte Updates möglich. Mit Control Manager können Produkte in Gruppen oder einzeln konfiguriert und verwaltet werden.

Die folgende Darstellung illustriert, wie Sie Endpoint Encryption zum ersten Mal verteilen und Control Manager zur Verwaltung von PolicyServer verwenden. In einer Control Manager Installation setzen Administratoren Control Manager für alle Endpoint Encryption Richtlinien, Benutzer und Gerätefunktionen ein und verwenden PolicyServer MMC nur für die erweiterte Unternehmenswartung.



Hinweis

In Umgebungen, in denen Control Manager eingesetzt wird, werden Änderungen an PolicyServer Richtlinien immer von Control Manager gesteuert. Alle mit PolicyServer MMC durchgeführten Änderungen werden beim nächsten Mal überschrieben, wenn Control Manager die Richtlinien mit der PolicyServer Datenbank synchronisiert.

Control Manager Architektur

Trend Micro Control Manager bietet Funktionen, um Produkte und Dienste von Trend Micro von einer zentralen Stelle aus zu steuern. Diese Anwendung vereinfacht die

Verwaltung der Viren/Malware- und Content-Sicherheitsrichtlinien im Unternehmen. Die folgende Tabelle enthält eine Liste der Komponenten, die von Control Manager verwendet werden.

TABELLE 3-1. Control Manager Komponenten

KOMPONENTE	BESCHREIBUNG
Control Manager server	Dient als ein Repository für alle Daten, die von den Agents erfasst werden. Dabei kann es sich um Server der Standard Edition oder der Advanced Edition handeln. Ein Control Manager Server unterstützt die folgenden Funktionen: • Eine SQL-Datenbank, in der die Konfigurationen und die Protokolle der verwalteten Produkte gespeichert werden. Control Manager arbeitet mit der Datenbank Microsoft SQL Server (`db_ControlManager.mdf`) zusammen, um Daten zu speichern, die in Protokollen, Communicator Zeitplänen, verwalteten Produkten und Informationen zu untergeordneten Servern, Benutzerkonten, Netzwerkumgebungen und Benachrichtigungseinstellungen enthalten sind. • Ein Webserver als Host für die Webkonsole von Control Manager. • Ein Mail-Server, der die Benachrichtigungen bei Ereignissen in Form von E-Mail-Nachrichten versendet. Control Manager kann Benachrichtigungen an Einzelpersonen oder Empfängergruppen über Ereignisse senden, die im Control Manager Netzwerk auftreten. In Event Center können Sie konfigurieren, ob Benachrichtigungen als E-Mail-Nachrichten, Windows Ereignisprotokoll, MSN Messenger, SNMP, Syslog, Pager oder an eine andere interne oder dem Branchenstandard entsprechende Anwendung gesendet werden, die von Ihrem Unternehmen zur Versendung von Benachrichtigungen eingesetzt wird. • Ein Berichtserver, der nur zum Umfang der Advanced Edition gehört, generiert Berichte zu Antiviren- und Content-Sicherheitsprodukten. Ein Control Manager Bericht ist eine Online-Sammlung von Zahlen über das Auftreten von Ereignissen zu Sicherheitsbedrohungen und Content-Sicherheit im Control Manager Netzwerk, die ein Sicherheitsrisiko darstellen.

KOMPONENTE	BESCHREIBUNG
Das Trend Micro Management Communication Protocol	MCP verarbeitet die Interaktion von Control Manager Server mit den verwalteten Produkten, die den Agent der nächsten Generation unterstützen. MCP ist das neue Rückgrat für das Control Manager System. MCP Agents werden mit den verwalteten Produkten installiert und nutzen eine Ein-Weg- oder Zwei-Wege-Kommunikation zur Kommunikation mit Control Manager. MCP Agents rufen Anweisungen und Updates vom Control Manager ab.
Trend Micro Management Infrastructure	Verarbeitet die Interaktion von Control Manager Server mit älteren verwalteten Produkten. Der Communicator bzw. das Message Routing Framework ist das Kommunikationsrückgrat für das ältere Control Manager System. Dabei handelt es sich um eine Komponente der Trend Micro Management Infrastructure (TMI). Communicators verarbeiten die gesamte Kommunikation zwischen dem Control Manager Server und den älteren verwalteten Produkten. Die Kommunikation mit den älteren verwalteten Produkten erfolgt durch Interaktion mit Control Manager 2.x Agents.
Control Manager 2.x Agents	Empfangen Befehle von Control Manager Server und senden Statusinformationen und Protokolle an den Control Manager Server Beim Control Manager Agent handelt es sich um eine Anwendung, die auf dem Server eines verwalteten Produkts installiert ist und die es möglich macht, dass Control Manager das Produkt verwaltet. Agents interagieren mit dem verwalteten Produkt und Communicator. Ein Agent dient als Brücke zwischen dem verwalteten Produkt und Communicator. Aus diesem Grund sollten Sie alle Agents auf demselben Computer wie die verwalteten Produkte installieren.

KOMPONENTE	BESCHREIBUNG
Webbasierte Management-Konsole	Ermöglicht, dass ein Administrator Control Manager von quasi jedem Computer mit einer Internet-Verbindung und Windows™ Internet Explorer™ aus verwaltet. Bei der Management-Konsole von Control Manager handelt es sich um eine Web-basierte Konsole, die im Internet über den Microsoft Internet Information Server (IIS) veröffentlicht wurde und die vom Control Manager Server gehostet wird. Mit dieser Lösung können Sie das Control Manager Netzwerk von einem beliebigen Computer verwalten, auf dem ein kompatibler Webbrowser verwendet wird.
Widget-Framework	Ermöglicht Administratoren, ein angepasstes Dashboard zur Überwachung des Control Manager Netzwerks zu erstellen.

Zusammenfassung der Vorgänge zum Konfigurieren von Control Manager

Das folgende Verfahren bietet eine Übersicht über die Konfiguration von Control Manager für die Endpoint Encryption Management.

Hinweis

Informationen über die Konfiguration einzelner Richtlinien finden Sie unter *Richtlinien in Control Manager auf Seite 5-1*.

Prozedur

1. Installieren und Konfigurieren von PolicyServer.

   Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

2. Verbinden Sie PolicyServer mit Control Manager.

   a. *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 3-8*

b. *Verzeichnisverwaltung für PolicyServer konfigurieren auf Seite 3-10*

3. Fügen Sie Richtlinienziele hinzu.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

4. Verifizieren Sie die Richtlinienkonfiguration auf PolicyServer MMC.

PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen

Endpoint Encryption ermöglicht, dass Administratoren PolicyServer mit Hilfe von Trend Micro Control Manager steuern und Endpoint Encryption Agent-Richtlinien verwalten, oder mit Trend Micro OfficeScan die Endpoint Encryption AgentSoftware auf verwaltete Endpunkte verteilen.

Wenn Sie Control Manager zur Verwaltung von PolicyServer verwenden möchten, müssen Sie PolicyServer als verwaltetes Produkt hinzufügen.

Vergewissern Sie sich bevor Sie fortfahren, dass die folgenden Aufgaben abgeschlossen wurden:

1. Installieren und Konfigurieren von Control Manager.

   Die begleitende Dokumentation finden Sie unter:

   http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

2. Installieren und Konfigurieren von PolicyServer.

   Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Wichtig

Endpoint Encryption unterstützt immer nur eine einzige konfigurierte PolicyServer Instanz in Control Manager. Es ist nicht möglich, mehrere PolicyServer Konfigurationen hinzuzufügen. Wenn Sie einen anderen PolicyServer konfigurieren möchten, müssen Sie zunächst den zuvor konfigurierten PolicyServer entfernen.

Prozedur

1. Überprüfen Sie alle Systemvoraussetzungen für kompatible Produktversionen.

   Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

2. Melden Sie sich bei Control Manager an.

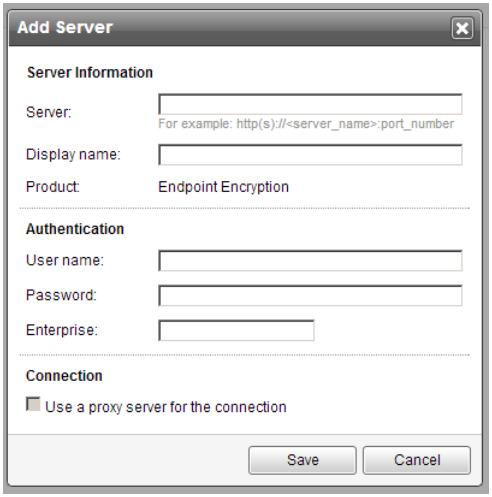
3. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

4. Wählen Sie im Listenfeld **Servertyp** die Option **Endpoint Encryption**.

5. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Server hinzufügen** wird angezeigt.



6. Geben Sie die Optionen für die **Serverinformationen** an.

   - **Server**: Geben Sie den Host-Namen und die Portnummer für PolicyServer an. Verwenden Sie das folgende Format:

     `http(s)://<Servername>:Portnummer`

Hinweis

Control Manager kommuniziert mit dem PolicyServer Endpoint Encryption Dienst. Die Standardportnummer lautet 8080.

- **Anzeigename:** Geben Sie an, wie PolicyServer im Fenster **Verwaltete Server** angezeigt wird.

7. Legen Sie unter **Authentifizierung** den Benutzernamen und das Kennwort für das Endpoint Encryption Unternehmensadministratorkonto fest.
8. Wählen Sie unter **Verbindung** den Eintrag **Einen Proxy-Server für die Verbindung verwenden**, wenn PolicyServer eine Proxy-Serververbindung erfordert.
9. Klicken Sie auf **Speichern**.

Hinweis

Die Synchronisierung zwischen Control Manager und PolicyServer dauert u. U. einige Minuten.

PolicyServer wird als neues verwaltetes Produkt zu Control Manager hinzugefügt.

Verzeichnisverwaltung für PolicyServer konfigurieren

Das folgende Verfahren erklärt die Konfiguration der Verzeichnisverwaltung für die Datenquelle des neuen PolicyServer. Beim Erstellen von Richtlinienzielen wird die Verzeichnisverwaltung in der Verzeichnisstruktur dargestellt. Detaillierte Hinweise zum Fenster **Verzeichnisverwaltung** finden Sie unter *Grundlegendes zum Produktverzeichnis auf Seite A-17*.

Stellen Sie sicher, dass PolicyServer als verwalteter Server zu Control Manager hinzugefügt wurde, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter *PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen auf Seite 3-8*.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Verwaltete Server**.

   Das Fenster **Verwaltete Server** wird angezeigt.

2. Klicken Sie auf **Verzeichnisverwaltung**.

   Das Fenster **Verzeichnisverwaltung** wird angezeigt.

3. Wählen Sie den Server, und klicken Sie anschließend auf **Ordner hinzufügen**.

   Das Fenster **Verzeichnis hinzufügen** wird angezeigt.

4. Geben Sie den Verzeichnisnamen an, und klicken Sie anschließend auf **Speichern**.

5. Klicken Sie zur Bestätigung auf **OK**.

   Der neue Ordner wird erstellt.

6. Ziehen Sie die zuvor hinzugefügte PolicyServer Datenquelle in den neuen Ordner.

7. Klicken Sie zur Bestätigung auf **OK**.

8. Klicken Sie auf **< Zurück**, um zum Fenster **Richtlinienverwaltung** zurückzukehren.

Eine Richtlinie erstellen

Das folgende Verfahren erklärt, wie Sie eine Control Manager Richtlinie konfigurieren, die sich auf Endpoint Encryption Benutzer und Geräte auswirkt.

Wichtig

Wenn Sie ein Benutzerkonto der Richtlinie hinzufügen möchten, vergewissern Sie sich, dass das Benutzerkonto bereits vorhanden ist.

Hinweis

Informationen zu den verfügbaren Richtlinieneinstellungen finden Sie unter *Endpoint Encryption Richtlinieneinstellungen auf Seite 5-14*.

Weitere Informationen zum Hinzufügen von Endpoint Encryption Benutzern finden Sie unter *Benutzer zu Endpoint Encryption hinzufügen auf Seite 6-4*.

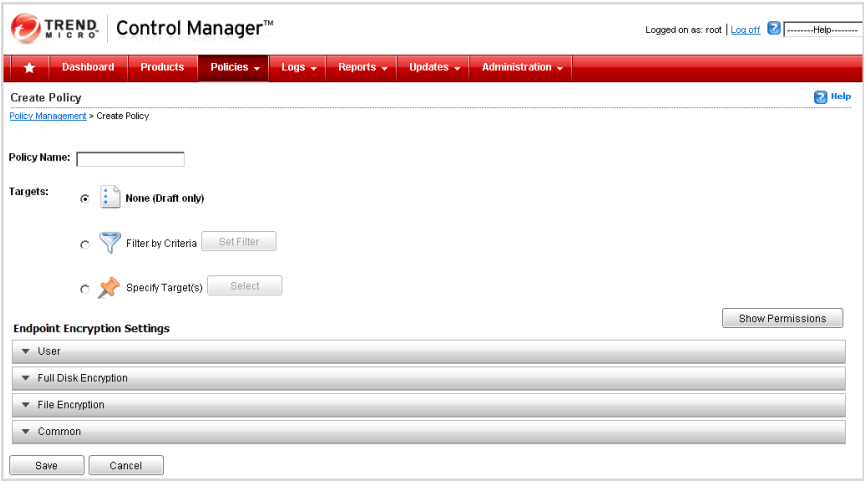
Informationen zur Konfiguration von Active Directory finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Informationen zur Richtlinienzuordnung zwischen Control Manager und PolicyServer MMC finden Sie unter *Richtlinienzuordnung zwischen Management-Konsolen auf Seite D-1*.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.
2. Wählen Sie im Listenfeld **Produkt** die Option **Endpoint Encryption**.
3. Klicken Sie auf **Erstellen**.

   Das Fenster **Richtlinie erstellen** wird angezeigt.



4. Geben Sie einen Richtliniennamen an.

5. Aktivieren Sie eine der folgenden Optionen für das Richtlinienziel:

   - **Keines (nur Entwurf)**: Sie erstellen eine Richtlinie ohne Ziele (Endpunkte).
   - **Filter nach Kriterien**: Endpoint Encryption unterstützt keine Filterung nach Kriterien.
   - **Ziel(e) angeben**: Sie geben vorhandene Endpunkte an.

   Hinweis

   Weitere Informationen über Richtlinienziele finden Sie unter *Richtlinienziele angeben auf Seite 3-14*.

6. Sie können die Richtlinieneinstellungen für Endpoint Encryption angeben.

   - Konfigurieren Sie **Benutzerrichtlinien**.

     Weitere Informationen finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

   - Konfigurieren Sie die Richtlinien für **Full Disk Encryption**.

Weitere Informationen finden Sie unter *Full Disk Encryption Regeln konfigurieren auf Seite 3-18*.

- Konfigurieren Sie die Richtlinien für **File Encryption**.

  Weitere Informationen finden Sie unter *File Encryption Regeln konfigurieren auf Seite 3-20*.

- Konfigurieren Sie die **allgemeinen Richtlinien**.

  Weitere Informationen finden Sie unter *Allgemeine Regeln für Richtlinien konfigurieren auf Seite 3-23*.

7. Klicken Sie auf **Speichern**.

Richtlinienziele angeben

Im Fenster **Ziel(e) angeben** weisen Sie die Endpoint Encryption Geräte der Richtlinie zu.

Hinweis

Das Fenster **Ziel(e) angeben** wird angezeigt, wenn Sie eine neue Richtlinie erstellen. Informationen zum Erstellen einer Richtlinie finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

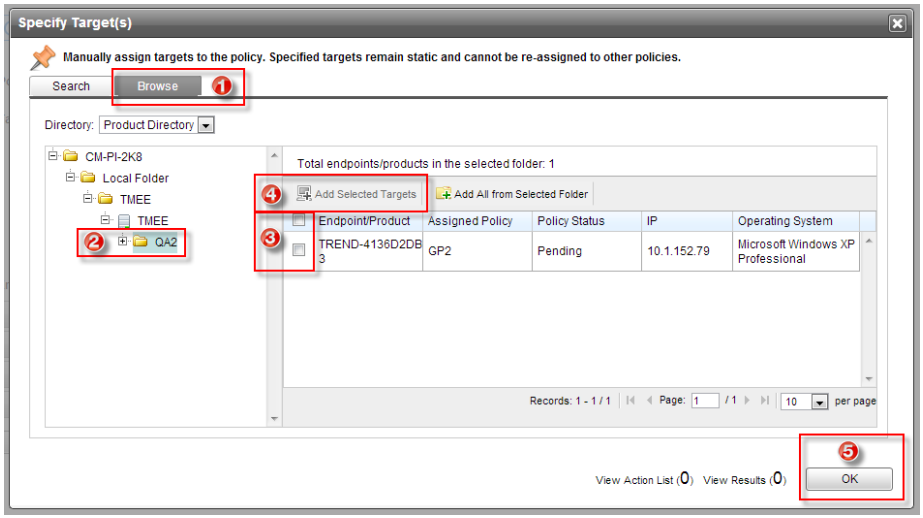


ABBILDUNG 3-1. Richtlinienziele angeben

Prozedur

1. Klicken Sie im Fenster **Ziel(e) angeben** auf die Registerkarte **Durchsuchen**.

2. Erweitern Sie die Struktur im linken Fensterbereich, um den verwalteten Ordner zu wählen.

   Beispiel: **CM-PI-2K8 > Lokaler Ordner > TMEE > TMEE > QA2**

3. Wählen Sie die entsprechenden Endpoint Encryption Geräte, oder aktivieren Sie das obere Kontrollkästchen, um alle Endpoint Encryption Geräte auszuwählen, die auf der aktuellen Seite aufgelistet werden.

4. Klicken Sie auf **Ausgewählte Ziele hinzufügen**.

Hinweis

Wenn Sie sofort alle Geräte im verwalteten Ordner auswählen möchten, klicken Sie auf **Alle aus ausgewähltem Ordner hinzufügen**.

„Aktionsliste anzeigen“ und „Ergebnisse anzeigen“ werden basierend auf der Auswahl aktualisiert.

5. Klicken Sie auf **OK**.

Regeln für Endpoint Encryption Benutzer konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die die Authentifizierung und Endpoint Encryption Benutzerkonten betreffen.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf **Benutzer**.

   Das Fenster zu den Richtlinienregeleinstellungen **Benutzer** wird angezeigt.

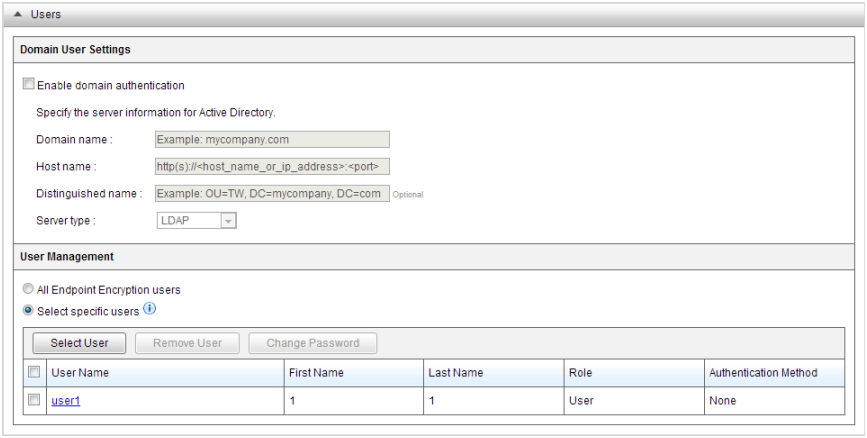


ABBILDUNG 3-2. Richtlinienregeln für Endpoint Encryption Benutzer

3. Wählen Sie unter **Domänenbenutzereinstellungen** die Option **Domänenauthentifizierung aktivieren**, um festzulegen, ob die Domänenauthentifizierung für Benutzer erforderlich ist.

Wichtig

Die Active Directory (AD) Synchronisierung erfordert, dass PolicyServer drei aktivierte Komponenten hat:

a. Konfigurieren Sie die AD-Domäne.

b. Lonfigurieren Sie die Richtliniengruppe, um auf die entsprechende Organisationseinheit (OU) zu verweisen.

c. Konfigurieren Sie die Richtliniengruppe mit entsprechenden Anmeldedaten für den Zugriff auf die AD-Domäne, die dem „Eindeutigen Namen“ der Richtliniengruppe entspricht.

Informationen zur Konfiguration der Domänenauthentifizierung finden Sie unter *PolicyServer - Active Directory-Synchronisierung* im *Endpoint Encryption Installations- und Migrationshandbuch*.

4. Konfigurieren Sie unter **Benutzerverwaltung** den Benutzerzugriff.

- Wählen Sie **Alle Benutzer von Endpoint Encryption**, um allen Benutzern, Domänen und lokalen Konten zu erlauben, Endpoint Encryption Geräte zu authentifizieren.
- Wählen Sie **Bestimmte Benutzer auswählen**, um festzulegen, welche bereits hinzugefügten Endpoint Encryption Benutzer sich an verwalteten Endpunkten authentifizieren können.

Hinweis

Richtlinienregeln wirken sich nur auf vorhandene Benutzerkonten aus. Vor der Konfiguration von Richtlinien können Sie neue Benutzer mit dem Widget "Endpoint Encryption Benutzer" hinzufügen. Weitere Informationen finden Sie unter *Benutzer zu Endpoint Encryption hinzufügen auf Seite 6-4*.

Full Disk Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf Full Disk Encryption Geräte auswirken.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf **Full Disk Encryption**.

Das Fenster mit den Einstellungen für **Full Disk Encryption** Richtlinienregeln wird angezeigt.

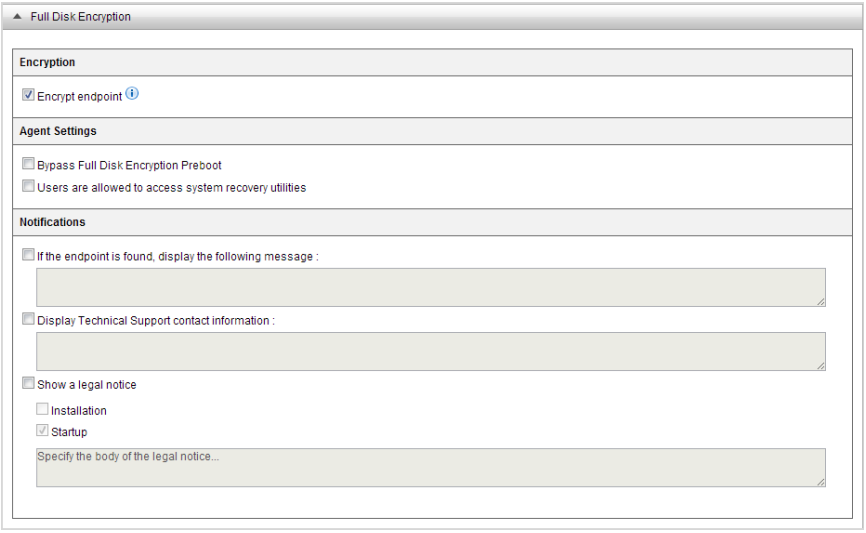


ABBILDUNG 3-3. Full Disk Encryption Richtlinienregeln

3. Wählen Sie unter **Verschlüsselung** die Option **Gerät verschlüsseln**, um eine Festplattenverschlüsselung zu starten, wenn der Endpoint Encryption Agent Richtlinien mit PolicyServer synchronisiert.

Warnung!

Sie sollten Full Disk Encryption Agents nicht verschlüsseln, ohne zuvor die Festplatte des Endpunkts vorzubereiten.

Informationen zur Vorbereitung der Festplatte finden Sie unter *Full Disk Encryption - Überblick über die Verteilung* im *Endpoint Encryption Installationshandbuch*.

4. Wählen Sie unter **Agent-Einstellungen** die folgenden Optionen:

   - Wählen Sie **Full Disk Encryption Preboot umgehen**, um dem Benutzer die Berechtigung zu geben, sich direkt bei Windows ohne den Schutz der Preboot-Authentifizierung zu authentifizieren.

- Wählen Sie **Benutzer sind berechtigt, auf die Systemwiederherstellungstools des Geräts zuzugreifen**, um Benutzern zu erlauben, auf die Wiederherstellungskonsole zuzugreifen.

  Informationen zu den konfigurierbaren Optionen und verfügbaren Tools in Full Disk Encryption finden Sie unter *Full Disk Encryption – Wiederherstellungskonsole auf Seite 14-21*.

5. Konfigurieren Sie die folgenden Optionen unter **Benachrichtigungen**:

   - Wählen Sie **Falls der Endpunkt gefunden wird, folgende Meldung anzeigen**, um eine Meldung anzuzeigen, wenn die Richtlinie **Falls gefunden** aktiv ist.
   - Wählen Sie **Kontaktdaten für den Technischen Support anzeigen**, um eine Meldung anzuzeigen, wenn sich der Benutzer am Full Disk Encryption Agent anmeldet.
   - Wählen Sie **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von Full Disk Encryption Agent anzuzeigen.

File Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf File Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf "File Encryption".

Das Fenster mit den Einstellungen für **File Encryption** Richtlinienregeln wird angezeigt.

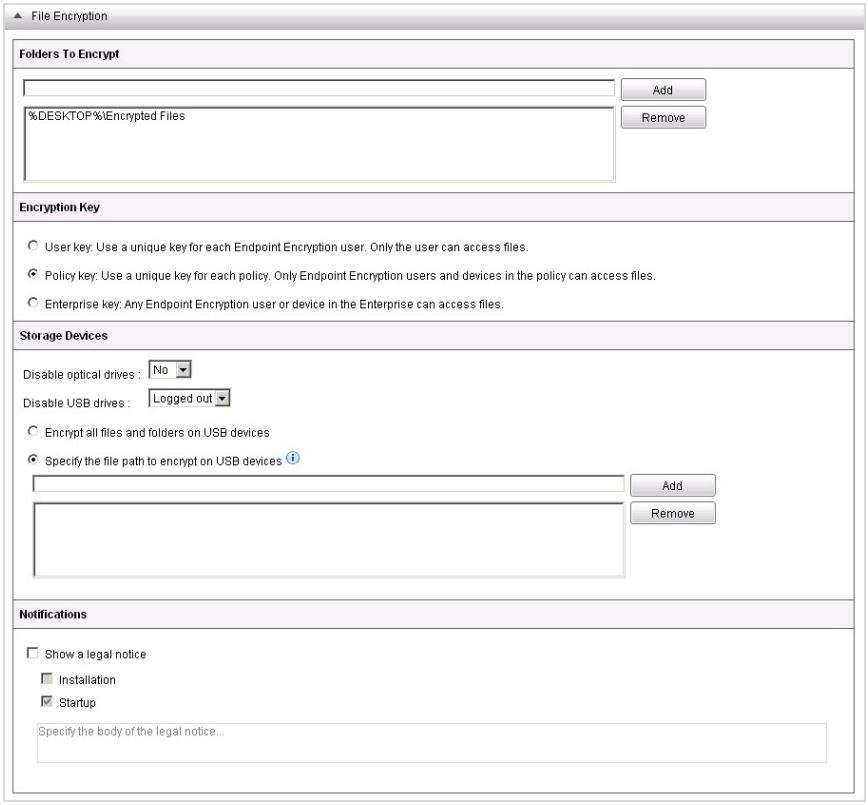

File Encryption
Folders To Encrypt
Add
%DESKTOP%\Encrypted Files
Remove
Encryption Key
User key: Use a unique key for each Endpoint Encryption user. Only the user can access files.
Policy key: Use a unique key for each policy. Only Endpoint Encryption users and devices in the policy can access files.
Enterprise key: Any Endpoint Encryption user or device in the Enterprise can access files.
Storage Devices
Disable optical drives :
No
Disable USB drives :
Logged out
Encrypt all files and folders on USB devices
Specify the file path to encrypt on USB devices
Add
Remove
Notifications
Show a legal notice
Installation
Startup
Specify the body of the legal notice...

ABBILDUNG 3-4. File Encryption Richtlinienregeln

3. Legen Sie unter **Zu verschlüsselnde Ordner** die Ordner fest, die auf dem Endpunkt automatisch erstellt und verschlüsselt werden, wenn der File Encryption Agent Richtlinien synchronisiert.

4. Wählen Sie unter **Verschlüsselungsschlüssel** die Verschlüsselung für den verschlüsselten File Encryption Ordner.

- **Benutzerschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jeden Endpoint Encryption Benutzer. Nur der Endpoint Encryption Benutzer kann Dateien entschlüsseln, die von ihm oder von ihr verschlüsselt wurden.
- **Richtlinienschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jede Richtlinie. Nur Endpoint Encryption Benutzer und Geräte in der Richtlinie können Dateien entschlüsseln.
- **Unternehmensschlüssel**: Alle Endpoint Encryption Benutzer oder Geräte im Unternehmen können Dateien entschlüsseln.

Hinweis

Durch die Auswahl von **Richtlinienschlüssel** oder **Unternehmensschlüssel** steuern Sie den Austausch des gemeinsamen Schlüssels für File Encryption. Weitere Informationen finden Sie unter *File Encryption Verschlüsselung mit gemeinsamem Schlüssel auf Seite 13-17*.

5. Konfigurieren Sie die folgenden Optionen unter **Speichergeräte**:
   - Wählen Sie **Optisches Laufwerk deaktivieren**, um festzulegen, ob der Zugriff auf Wechselmedien vom Endpunkt aus möglich ist.
   - Wählen Sie **USB-Laufwerk deaktivieren**, um festzulegen, ob USB-Ports deaktiviert sind. Folgende Optionen sind möglich:
     - **Immer**
     - **Abgemeldet**
     - **Nie**
   - Wählen Sie **Alle Dateien und Ordner auf USB-Geräten verschlüsseln**, um automatisch alle Dateien und Ordner auf Wechselmedien zu verschlüsseln, wenn diese mit dem Endpunkt verbunden sind.
   - Wählen Sie **Zu verschlüsselnden Dateipfad auf USB-Geräten angeben**, um verschlüsselte Ordner auf USB-Laufwerken hinzuzufügen oder zu entfernen. Nicht vorhandene Ordner werden erstellt. Wenn kein Laufwerksbuchstabe angegeben wird, gilt diese Regel für alle USB-Geräte.

6. Wählen Sie unter **Benachrichtigungen** die Option **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von File Encryption Agent anzuzeigen.

Allgemeine Regeln für Richtlinien konfigurieren

In diesem Abschnitt werden die konfigurierbaren Optionen für Richtlinienregeln erläutert, die sich auf alle Endpoint Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf **Allgemein**.

Das Fenster zu den Richtlinienregeleinstellungen **Allgemein** wird angezeigt.

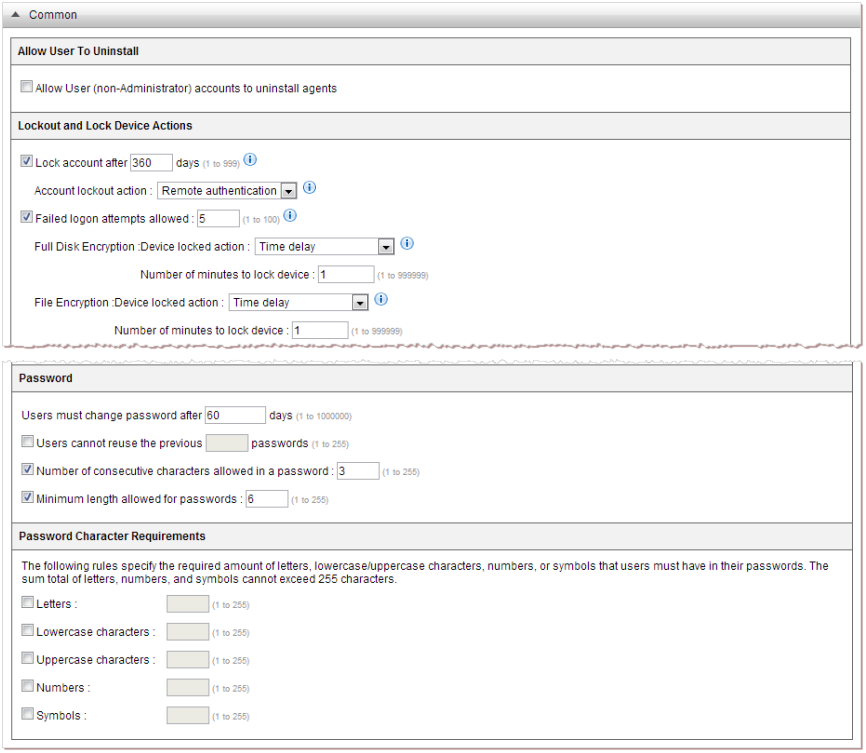

Common
Allow User To Uninstall
Allow User (non-Administrator) accounts to uninstall agents
Lockout and Lock Device Actions
Lock account after 360 days (1 to 999)
Account lockout action : Remote authentication
Failed logon attempts allowed : 5 (1 to 100)
Full Disk Encryption :Device locked action : Time delay
Number of minutes to lock device : 1 (1 to 999999)
File Encryption :Device locked action : Time delay
Number of minutes to lock device : 1 (1 to 999999)
Password
Users must change password after 60 days (1 to 1000000)
Users cannot reuse the previous passwords (1 to 255)
Number of consecutive characters allowed in a password : 3 (1 to 255)
Minimum length allowed for passwords : 6 (1 to 255)
Password Character Requirements
The following rules specify the required amount of letters, lowercase/uppercase characters, numbers, or symbols that users must have in their passwords. The sum total of letters, numbers, and symbols cannot exceed 255 characters.
Letters : (1 to 255)
Lowercase characters : (1 to 255)
Uppercase characters : (1 to 255)
Numbers : (1 to 255)
Symbols : (1 to 255)

ABBILDUNG 3-5. Allgemeine Richtlinienregeln

3. Wählen Sie unter **Deinstallation durch Benutzer zulassen** die Option **Nicht-Administratorkonten können die Agent-Software deinstallieren**, um allen Endpoint Encryption Benutzern zu erlauben, den Agent zu deinstallieren.

Hinweis

Standardmäßig können nur Unternehmensadministratoren Endpoint Encryption Agents deinstallieren.

4. Konfigurieren Sie unter **Aktionen zum Sperren von Geräten** die folgenden Optionen:

- Wählen Sie **Konto sperren nach <Anzahl> Tage**, um die Anzahl der Tage anzugeben, nach denen das Endpoint Encryption Gerät gesperrt wird, wenn die Richtlinien nicht synchronisiert werden.

  - Geben Sie mit **Kontosperraktion** an, ob bei einer Sperrung die Remote-Authentifizierung oder Löschung aktiviert werden soll.

    Hinweis

    Weitere Informationen zu den Sperroptionen finden Sie unter *Aktionen zum Sperren von Konten und Geräten auf Seite 3-26*.

- Wählen Sie **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**, um anzugeben, wie viele Authentifizierungsversuche möglich sind, bevor das Endpoint Encryption Gerät gesperrt wird.

- Konfigurieren Sie für Full Disk Encryption oder File Encryption Geräte Folgendes separat:

  - Geben Sie mit **Aktion zur Gerätesperrung** an, ob bei einer Sperrung die „Remote-Authentifizierung“ oder die „Löschung“ aktiviert werden soll.

    Hinweis

    Weitere Informationen zu den Sperroptionen finden Sie unter *Aktionen zum Sperren von Konten und Geräten auf Seite 3-26*.

  - Geben Sie unter **Anzahl der Minuten, die das Gerät gesperrt wird** die Dauer der Zeitverzögerung an, die das Endpoint Encryption Gerät gesperrt ist und nicht authentifiziert werden kann.

5. Konfigurieren Sie unter **Kennwort** die folgenden Optionen:

   - Wählen Sie **Benutzer muss das Kennwort nach <Anzahl> Tagen ändern**, um anzugeben, wenn ein Benutzer aufgefordert wird, das Kennwort zu aktualisieren.

   - Wählen Sie **Benutzer darf die vorherigen <Anzahl> Kennwörter nicht wiederverwenden**, um anzugeben, wie viele vorherige Kennwörter der Benutzer nicht verwenden darf.

- Wählen Sie **Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort**, um anzugeben, wie viele gleiche Zeichen ein Kennwort enthalten darf.
- Wählen Sie **Zulässige Mindestlänge für Kennwörter**, um anzugeben, aus wie vielen Zeichen ein Kennwort mindestens bestehen muss.

6. Legen Sie unter **Kennwortvoraussetzungen** die Einschränkungen in Bezug auf Zeichen in Kennwörtern fest.
   - **Buchstaben**
   - **Kleinbuchstaben**
   - **Großbuchstaben**
   - **Zahlen**
   - **Symbole**

Wichtig

Die Gesamtzahl der Buchstaben, Ziffern und Symbole kann höchstens 255 betragen.

Aktionen zum Sperren von Konten und Geräten

Einige Richtlinien verfügen über Einstellungen zum Sperren eines Benutzerkontos oder eines Geräts auf Grundlage bestimmter Kriterien. Aktionen zur Konto- oder Gerätesperrung wirken sich auf das Endpoint Encryption Gerät aus, unabhängig davon, ob der Agent die Richtlinien mit PolicyServer synchronisiert. Wenn ein Agent beispielsweise für eine bestimmte Zeitdauer nicht mit PolicyServer kommuniziert, sperrt der Endpoint Encryption Agent automatisch das Endpoint Encryption Gerät. Die nachfolgende Tabelle vermittelt Ihnen ein Verständnis der verfügbaren Aktionen zur Sperrung von Konten und Geräten.

TABELLE 3-2. Kontosperraktionen

AKTION	BESCHREIBUNG
Remote-Authentifizierung	Benutzer können sich so lange nicht am Endpoint Encryption Gerät anmelden, bis der Technische Support Unterstützung zur Remote-Authentifizierung bereitstellt.
Löschen	Wenn der Agent das nächste Mal die Richtlinien synchronisiert, werden alle Daten gelöscht.

Hinweis

Kontosperraktionen werden wirksam, wenn der Endpoint Encryption Agent innerhalb eines bestimmten Zeitraums (der durch die Richtlinie festgelegt wird) nicht mit PolicyServer kommuniziert.

TABELLE 3-3. Gerätesperraktionen

AKTION	BESCHREIBUNG
Löschen	Wenn der Endpoint Encryption Agent das nächste Mal die Richtlinien synchronisiert, werden alle Daten gelöscht.
Remote-Authentifizierung	Benutzer können sich so lange nicht an den Endpoint Encryption Geräten anmelden, bis der Technische Support Unterstützung zur Remote-Authentifizierung bereitstellt.
Zeitverzögerung	Benutzer können sich für eine bestimmte Zeitdauer nicht an den Endpoint Encryption Geräten anmelden.

Hinweis

Gerätesperraktionen werden wirksam, wenn der Endpoint Encryption Benutzer zu häufig erfolglos versucht hat, sich am Endpoint Encryption Gerät anzumelden (die Häufigkeit wird in der Richtlinie festgelegt).

Richtlinienregeln für die Remote-Hilfe

In der folgenden Tabelle werden die Speicherorte der Richtlinien für die Konten- und Gerätesperrung beschrieben, die sich auf die Remote-Hilfe-Authentifizierung auswirken.

Diese Informationen vermitteln ein Verständnis dafür, welche Richtlinien festgelegt werden sollten.

TABELLE 3-4. Richtlinienspeicherorte für die Remote-Hilfe

NAME DER RICHTLINIE	MENÜPFAD FÜR POLICYSERVER MMC	MENÜPFAD FÜR CONTROL MANAGER	BESCHREIBUNG
Kontosperraktion	**Anmelden** > **Kontosperraktion**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Kontosperraktion**	Die Maßnahme, die durchgeführt wird, nachdem die Zeitdauer in „Kontosperraktionen “ abgelaufen ist. Mögliche Maßnahmen sind: Löschen, Remote-Authentifizierung
Zeitraum bis Kontosperrung	**Anmelden** > **Zeitraum bis Kontosperrung**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Konto sperren nach [ ] Tagen**	Die Anzahl von Tagen, die ein Gerät ohne Kommunikation mit PolicyServer sein kann, bevor die „Kontosperraktion“ ausgeführt wird.
Aktion zur Gerätesperrung	Für jeden Agent: **Anmelden** > **Aktion zur Gerätesperrung**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Aktion zur Gerätesperrung**	Die Aktion, die durchgeführt wird, wenn der in der Richtlinie „Zulässige Anzahl fehlgeschlagener Anmeldeversuche“ festgelegte Wert überschritten wurde. Unterstütze Maßnahmen: Zeitverzögerung, Löschen, Remote-Authentifizierung

Name der Richtlinie	Menüpfad für PolicyServer MMC	Menüpfad für Control Manager	Beschreibung
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Für jeden Agent: **Anmelden** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche, bevor die Aktion zur „Gerätesperrung“ ausgeführt wird.

Kapitel 4

Dashboard, Widgets und Berichte

In diesem Kapitel werden die Verwendung von Control Manager Dashboard, die Verwaltung von Widgets und die Ausführung von Berichten beschrieben.

Es werden folgende Themen behandelt:

- *Das Dashboard verwenden auf Seite 4-2*
- *Grundlegendes zu Registerkarten auf Seite 4-2*
- *Grundlegendes zu Widgets auf Seite 4-5*
- *Endpoint Encryption Widgets verwenden auf Seite 4-9*

Das Dashboard verwenden

Das Control Manager Dashboard bietet Informationen für das Control Manager Netzwerk, die auf einen Blick abgelesen werden können. Das Dashboard besteht aus zwei Komponenten:

- **Tabs:** Ermöglicht Administratoren, ein Fenster zu erstellen, das mindestens ein Widget enthält.
- **Widgets:** Liefern spezielle Informationen über unterschiedliche sicherheitsrelevante Ereignisse.

Benutzerkonten und das Dashboard

Für jedes Benutzerkonto wird ein eigenes Dashboard angezeigt. Wenn sich ein Benutzer zum ersten Mal bei Control Manager anmeldet, werden die Standardregisterkarten und -Widgets innerhalb der Registerkarten auf dem Dashboard angezeigt.

Das Dashboard, die Registerkarten und die Widgets können für jedes Benutzerkonto und die entsprechenden speziellen Anforderungen angepasst werden. Die Anpassung von Dashboard, Registerkarten oder Widgets für ein Benutzerkonto wirkt sich nicht auf das Dashboard, die Registerkarten oder die Widgets anderer Benutzerkonten aus. Jedes Benutzerkonto verfügt über ein Dashboard sowie Registerkarten und Widgets, die von jedem anderen Benutzerkonto komplett unabhängig sind.

Grundlegendes zu Registerkarten

Sie können das Control Manager Dashboard anpassen, indem Sie zusätzliche Registerkarten hinzufügen, den neuen Registerkarten Namen nach Bedarf geben und die entsprechenden Widgets ergänzen. Sie können hinzugefügte Registerkarten ändern oder löschen.

Standardregisterkarten

Das Dashboard enthält die folgenden Registerkarten:

- Zusammenfassung
- Untersuchung von DLP-Vorfällen
- Prävention vor Datenverlust
- Einhaltung von Richtlinien
- Bedrohungserkennung
- Smart Protection Network

Hinweis

Wenn Sie die Standardregisterkarten endgültig löschen, werden die Registerkarten nicht mehr für das Benutzerkonto angezeigt, das die Registerkarten entfernt hat. Es gibt keine Möglichkeit, eine gelöschte Registerkarte wiederherzustellen. Das Löschen einer Standardregisterkarte hat für andere Benutzerkonten keine Auswirkung auf die Anzeige des Dashboards.

Neue Registerkarte hinzufügen

Prozedur

1. Navigieren Sie zum **Dashboard**.
2. Klicken Sie rechts neben der letzten benannten Registerkarte auf +.

   Das Fenster **Neue Registerkarte** wird angezeigt.
3. Geben Sie einen Namen für den **Titel** der neuen Registerkarte ein.
4. Aktivieren Sie das Optionsfeld für den entsprechenden Layout-Stil.
5. Wählen Sie **Automatisch anpassen Ein**, um die Höhe der Widgets entsprechend der Registerkarte festzulegen.
6. Klicken Sie auf **Speichern**.

Die neue Registerkarte wird rechts neben den vorhandenen Registerkarten hinzugefügt.

Registerkarteneinstellungen ändern

Prozedur

1. Navigieren Sie zu **Dashboard**, und öffnen Sie anschließend die entsprechende Registerkarte.
2. Klicken Sie auf **Registerkarteneinstellungen** in der oberen rechten Ecke der Registerkarte.
3. Nehmen Sie die erforderlichen Änderungen vor:
   - **Titel**
   - **Layout**
   - **Automatisch anpassen**
4. Klicken Sie auf **Speichern**.

Eine Registerkarte löschen

Hinweis

Wenn Sie die Standardregisterkarten endgültig löschen, werden die Registerkarten nicht mehr für das Benutzerkonto angezeigt, das die Registerkarten entfernt hat. Es gibt keine Möglichkeit, eine gelöschte Registerkarte wiederherzustellen. Das Löschen einer Standardregisterkarte hat für andere Benutzerkonten keine Auswirkung auf die Anzeige des Dashboards.

Prozedur

1. Navigieren Sie zum **Dashboard**.
2. Öffnen Sie die Registerkarte, die gelöscht werden soll.
3. Klicken Sie auf das **X** neben dem Namen der Registerkarte.
4. Klicken Sie zur Bestätigung auf **OK**.

Die Registerkarte wird gelöscht.

Grundlegendes zu Widgets

Widgets sind die Hauptkomponenten des Dashboards. Registerkarten stellen das Layout und Widgets die tatsächlichen Daten für das Dashboard bereit.

Hinweis

Die Anpassung von Dashboard, Registerkarten oder Widgets für ein Benutzerkonto wirkt sich nicht auf das Dashboard, die Registerkarten oder die Widgets anderer Benutzerkonten aus. Jedes Benutzerkonto verfügt über ein Dashboard sowie Registerkarten und Widgets, die von jedem anderen Benutzerkonto komplett unabhängig sind.

Laden Sie den Control Manager Widget-Pool (unter **Product programs and widget pool** in den Fenstern **Manual Download** und **Scheduled Download**) regelmäßig herunter, um zu überprüfen, ob neue und aktualisierte Widgets vorliegen.

Die Daten, die auf einem Widget angezeigt werden, stammen aus den folgenden Quellen:

- Control Manager Datenbank
- Trend Micro Smart Protection Network
- Verwaltete Produkte, die der Dashboard-Liste **Server Visibility** hinzugefügt wurden

Hinweis

Smart Feedback muss aktiviert werden, um Daten für Widgets anzuzeigen, die Daten aus dem Smart Protection Network enthalten.

Die auf einem Widget angezeigten Daten werden auf zweierlei Art gesteuert:

TABELLE 4-1. Widget-Informationen

VORGANG	DETAILS
Benutzerkonto	Ein Benutzerkonto gewährt oder beschränkt den Zugang zu allen verwalteten Produkten, die in Control Manager registriert sind.
Bereich	Der Geltungsbereich der Daten auf vielen Widgets kann individuell konfiguriert werden. Das bedeutet, ein Benutzer kann ferner den Speicherort der Datenquelle für das Widget angegeben. **Beispiel:** Ein OfficeScan Administrator, der mehrere OfficeScan Server verwaltet, kann eine Registerkarte anlegen und Widgets hinzufügen, die nur Daten für einen OfficeScan Server anzeigen.

Widgets zu einer Registerkarte hinzufügen

Nachdem Sie Widgets einer Registerkarte hinzugefügt haben, können Sie das Widget an verschiedene Positionen innerhalb der Registerkarte ziehen. Informationen zum Anpassen von Widgets finden Sie unter *Widgets anpassen auf Seite 4-7*.

Prozedur

1. Navigieren Sie zu **Dashboard**, und öffnen Sie anschließend die entsprechende Registerkarte.
2. Klicken Sie auf **Widgets hinzufügen** in der oberen rechten Ecke der Registerkarte.

   Das Fenster **Widgets hinzufügen** wird angezeigt.
3. Gehen Sie folgendermaßen vor:
   - Klicken Sie auf der linken Seite auf eine Kategorie, und aktivieren Sie anschließend das Kontrollkästchen neben dem Namen aller entsprechenden Widgets, die angezeigt werden.
   - Wählen Sie mit Hilfe der Suchleiste ein bestimmtes Widget.
4. Klicken Sie auf **Hinzufügen**.

Alle ausgewählten Widgets werden der Registerkarte hinzugefügt.

Widgets anpassen

Sie können die in einem Widget angezeigten Informationen manuell aktualisieren, konfigurieren oder filtern. Es ist ebenfalls möglich, Informationen über einen bestimmten Zeitraum anzuzeigen. Einige Widgets stellen die Daten in Form eines Diagramms oder einer Tabelle dar.

Informationen zu weiteren Anpassungen finden Sie unter *Widget-Optionen auf Seite 4-8* oder *Endpoint Encryption Widgets verwenden auf Seite 4-9*.

Prozedur

1. Navigieren Sie zu **Dashboard**, und öffnen Sie anschließend die entsprechende Registerkarte.
2. Klicken Sie in der oberen linken Ecke des Widgets auf die Zeitangabe.
3. Bei einigen Widgets können Sie das Format zur Anzeige der Informationen auswählen. Klicken Sie dazu in der oberen rechten Ecke des Widgets auf das Diagramm- oder Listensymbol.
4. Bei einigen Widgets können Sie auf die Legende am unteren Rand des Widgets klicken, um die Informationen zu filtern.

Widget-Optionen

Die folgende Darstellung und Tabelle vermitteln einen allgemeinen Überblick über die verfügbaren Widget-Optionen. Unterschiedliche Widgets können unterschiedliche Optionen haben.

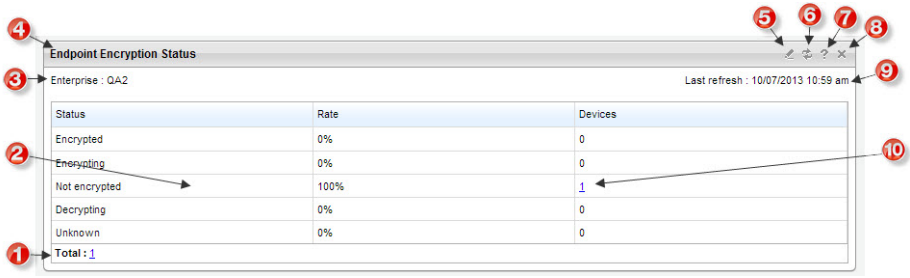


ABBILDUNG 4-1. Widget-Optionen

TABELLE 4-2. Beschreibungen der Widget-Optionen

VORGANG	BESCHREIBUNG
1	Die Gesamtzahl der Objekte (Beispiele: Ereignisse, Geräte, Protokolle), über die das Widget Daten sammelt. Klicken Sie auf die Zahl, um weitere Informationen anzuzeigen.
2	Die Informationen, die vom Widget angezeigt werden.
3	Das Unternehmen, das den Widget-Daten zugeordnet ist.
4	Der Name des Widgets. Wenn Sie den Namen ändern möchten, klicken Sie auf das -Symbol, um die Optionen des Widgets zu konfigurieren.
5	Klicken Sie auf das -Symbol, um für das Widget die Optionen zu konfigurieren, die angezeigt werden. Jedes Widget verfügt über andere Konfigurationsoptionen.

VORGANG	BESCHREIBUNG
6	Klicken Sie auf das -Symbol, um die Widget-Daten manuell zu aktualisieren. Die Standardaktualisierungsrate wird von den Control Manager Dashboard-Einstellungen bestimmt, die Sie unter **Administration** > **Einstellungen** > **Einstellungen der Webkonsole** festlegen.
7	Klicken Sie auf das -Symbol, um auf die Endpoint Encryption Online-Hilfe für das Widget zuzugreifen.
8	Klicken Sie auf das -Symbol, um das Widget zu schließen.
9	Hier sehen Sie, wann das Widget zum letzten Mal eine Datenaktualisierung durchgeführt hat.
10	Klicken Sie auf die Zahl oder das Symbol, um auf bestimmte Widget-Daten zuzugreifen, z. B. Ereignisprotokolle oder Berichte.

Widgets löschen

Prozedur

1. Navigieren Sie zu **Dashboard**, und öffnen Sie anschließend die entsprechende Registerkarte.
2. Klicken Sie in der oberen rechten Ecke des Widgets auf das Symbol .

Hinweis

Informationen zu den verfügbaren Optionen für Widgets finden Sie unter *Widget-Optionen auf Seite 4-8*.

Endpoint Encryption Widgets verwenden

Control Manager verfügt über mehrere Endpoint Encryption Widgets zur Verwaltung von Benutzern, Geräten und Berichten. Die folgenden Widgets sind verfügbar:

- *Widget Endpoint Encryption Benutzer auf Seite 4-10*
- *Widget Endpoint Encryption - Geräte auf Seite 4-12*
- *Widget "Full Disk Encryption Status" auf Seite 4-15*
- *Widget Erfolglose Anmeldeversuche am Endpoint Encryption Gerät auf Seite 4-18*
- *Widget Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers auf Seite 4-20*
- *Widget Endpoint Encryption Gerätesperrung auf Seite 4-23*
- *Widget Endpoint Encryption - Bericht zu Sicherheitsverstößen auf Seite 4-25*

Widget Endpoint Encryption Benutzer

Das Widget **Endpoint Encryption Benutzer** stellt Funktionen für die Benutzerverwaltung direkt vom Dashboard von Control Manager bereit. Mit dem Widget **Endpoint Encryption Benutzer** fügen Sie Endpoint Encryption Benutzerkonten hinzu oder entfernen sie, setzen Kennwörter zurück, ändern Berechtigungen, konfigurieren die Priorität der Richtliniengruppen, importieren aus Active Directory und suchen nach bestimmten Benutzerkonten.

Hinweis

Informationen zur Verwaltung von Benutzern mit dem Widget **Endpoint Encryption Benutzer** finden Sie unter *Benutzer in Control Manager auf Seite 6-1*.

Informationen, wie Sie vorhandene Endpoint Encryption Benutzer zu einer Richtlinie hinzufügen, finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

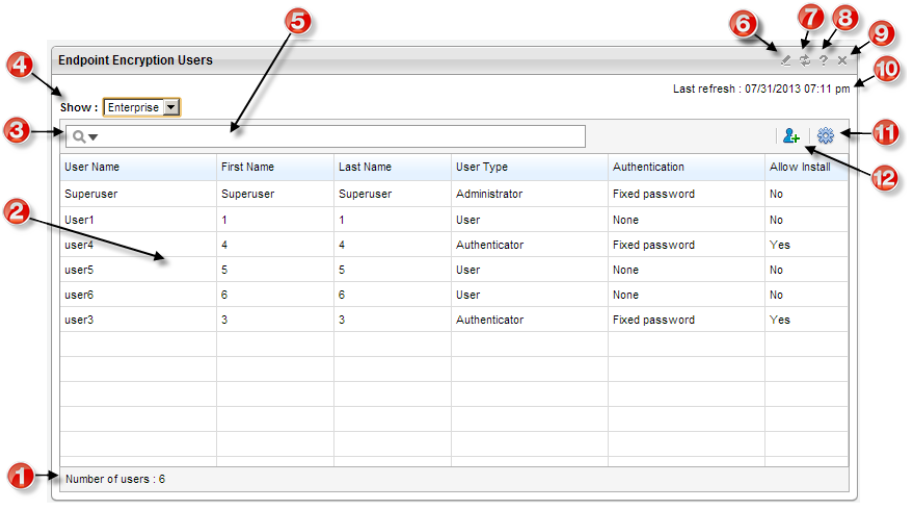


ABBILDUNG 4-2. Widget Endpoint Encryption Benutzer

TABELLE 4-3. Beschreibung des Widgets Endpoint Encryption Benutzer

VORGANG	BESCHREIBUNG
1	Zeigt die Gesamtzahl der Benutzer im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.
2	Alle Benutzer im Unternehmen, der ausgewählten Richtlinie oder der angegebenen Suche.
3	Klicken Sie auf das -Symbol, um zu filtern, welche Endpoint Encryption Benutzer in der Tabelle angezeigt werden.
4	Klicken Sie auf das Listenfeld **Anzeigen**, um das Unternehmen oder eine bestimmte Richtlinie auszuwählen, die in der Tabelle angezeigt wird.
5	Über das Suchfeld legen Sie Parameter für die Suche fest.
6	Klicken Sie auf das -Symbol, um die Widget-Einstellungen zu konfigurieren.
7	Klicken Sie auf das -Symbol, um die Widget-Daten zu aktualisieren.

VORGANG	BESCHREIBUNG
8	Klicken Sie auf das ?-Symbol, um die Online-Hilfe anzuzeigen.
9	Klicken Sie auf das -Symbol, um das Widget zu schließen.
10	Zeigen Sie an, wann das Widget zum letzten Mal Daten mit PolicyServer synchronisiert hat.
11	Klicken Sie auf das -Symbol, um die Benutzerattribute anzuzeigen oder Aktionen für einen beliebigen ausgewählten Benutzer auszuführen.
12	Klicken Sie auf das -Symbol, um einzelne Benutzer hinzuzufügen oder um Benutzer aus einer CSV-Datei oder aus Active Directory LDAP zu importieren.

Widget Endpoint Encryption - Geräte

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die bei PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

Das Widget **Endpoint Encryption - Geräte** stellt direkt im Dashboard von Control Manager Funktionen für die Endpoint Encryption Geräteverwaltung bereit. Mit dem Widget **Endpoint Encryption - Geräte** überwachen Sie Aktivitäten, suchen nach Endpoint Encryption Geräten oder sichern die Daten auf dem Endpunkt, indem Sie einen Befehl zum Sperren oder Löschen einleiten, wenn ein Endpunkt gestohlen wird oder verloren geht.

Hinweis

Informationen zur Verwaltung von Geräten mit dem Widget **Endpoint Encryption - Geräte** finden Sie unter *Geräte in Control Manager auf Seite 7-1*.

Informationen, wie Sie Endpoint Encryption Geräte zu einer Richtlinie hinzufügen, finden Sie unter *Richtlinienziele angeben auf Seite 3-14*.

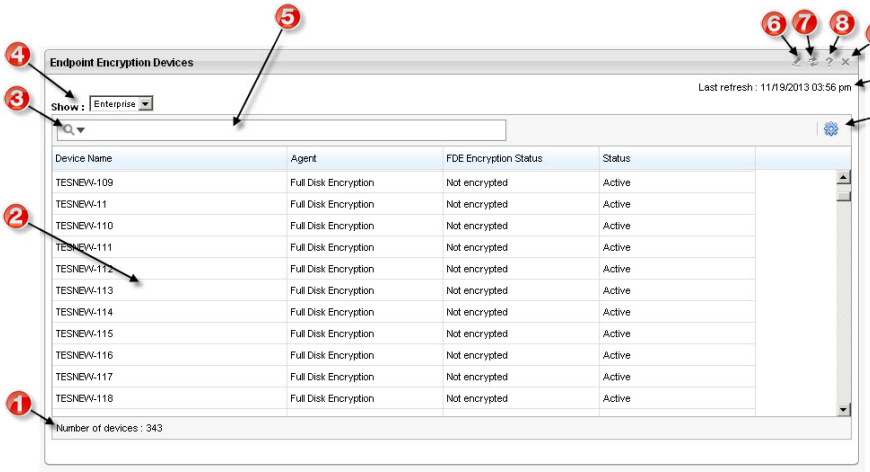


ABBILDUNG 4-3. Widget Endpoint Encryption - Geräte

TABELLE 4-4. Beschreibung des Widgets Endpoint Encryption - Geräte

VORGANG	BESCHREIBUNG
1	Zeigt die Gesamtzahl der Geräte im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.
2	Zeigt alle Geräte im gesamten Unternehmen, der ausgewählten Gruppe oder der angegebenen Suche an. • **Gerätename**: Der Computername, der dem Endpoint Encryption Gerät zugeordnet ist. • **Agent**: Der installierte Endpoint Encryption Agent. • **FDE Verschlüsselungsstatus**: Wenn Full Disk Encryption Agent installiert ist, der Verschlüsselungsstatus. Weitere Informationen finden Sie unter *Widget "Full Disk Encryption Status" auf Seite 4-15*. • **Status**: Der aktuelle Status des Endpoint Encryption Geräts.
3	Klicken Sie auf das Symbol, um den Endpoint Encryption Agent auszuwählen und die in der Tabelle angezeigten Geräte zu filtern.

VORGANG	BESCHREIBUNG
4	Klicken Sie auf das Listenfeld **Anzeigen**, um das gesamte Unternehmen oder eine bestimmte Richtlinie auszuwählen, die in der Tabelle angezeigt wird.
5	Über das Suchfeld legen Sie Parameter für die Suche fest. Sie können nach allen Attributen suchen, die in den Geräteattributen aufgeführt werden.
6	Klicken Sie auf das -Symbol, um die Widget-Einstellungen zu konfigurieren.
7	Klicken Sie auf das -Symbol, um die Widget-Daten zu aktualisieren.
8	Klicken Sie auf das -Symbol, um die Online-Hilfe anzuzeigen.
9	Klicken Sie auf das -Symbol, um das Widget zu schließen.
10	Zeigen Sie an, wann das Widget zum letzten Mal Daten mit PolicyServer synchronisiert hat.
11	Klicken Sie auf das -Symbol, um die Geräteattribute anzuzeigen oder Aktionen für ein beliebiges ausgewähltes Gerät auszuführen.

Widget "Full Disk Encryption Status"

Im Widget **Full Disk Encryption Status** wird der aktuelle Verschlüsselungsstatus aller Endpoint Encryption Geräte im Unternehmen angezeigt.

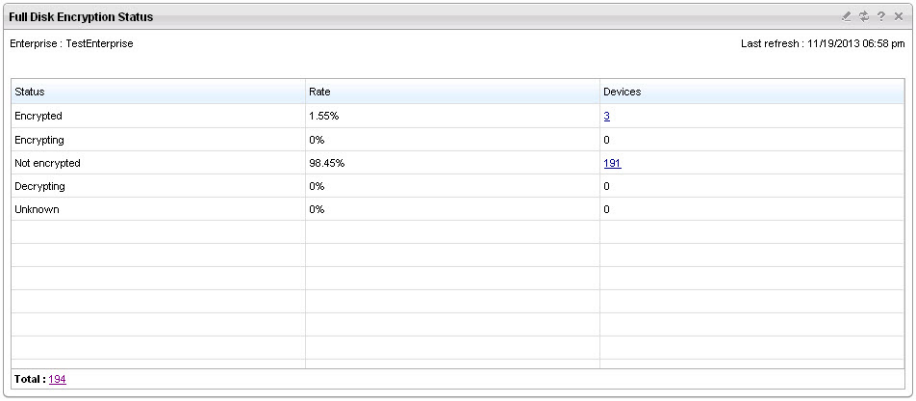


ABBILDUNG 4-4. Widget Full Disk Encryption Status

TABELLE 4-5. Beschreibung des Widgets Full Disk Encryption Status

SPALTE	BESCHREIBUNG
Status	Der Status des Endpoint Encryption Geräts. Enthaltene Statusangaben: • **Verschlüsselt**: Das Endpoint Encryption Gerät ist zu 100 % verschlüsselt. • **Verschlüsselung**: Die Festplatte des Endpoint Encryption Geräts wird momentan verschlüsselt. Der Status ändert sich in „Vollständig verschlüsselt“, sobald die Verschlüsselung abgeschlossen ist und der Endpunkt neu gestartet wird. • **Nicht verschlüsselt**: Das Endpoint Encryption Gerät ist zu 0% verschlüsselt. • **Entschlüsseln**: Die Festplatte des Endpoint Encryption Geräts wird momentan entschlüsselt. Der Status ändert sich in "Nicht verschlüsselt", sobald die Entschlüsselung abgeschlossen ist und der Endpunkt neu gestartet wird. • **Unbekannt**: Das Endpoint Encryption Gerät ist synchronisiert, jedoch kann PolicyServer den Verschlüsselungsstatus nicht ermitteln.
Rate	Der Prozentsatz der Verschlüsselung auf dem Endpoint Encryption Gerät.
Geräte	Die Anzahl der Endpoint Encryption Geräte mit dem aktuellen Status. Klicken Sie auf die Zahl, um den Bericht zu den Endpoint Encryption Geräten anzuzeigen. Weitere Informationen finden Sie unter *Bericht Full Disk Encryption Status auf Seite 4-16*.

Hinweis

Klicken Sie unten im Widget auf die Zahl neben **Gesamt**, um den Endpoint Encryption Statusbericht anzuzeigen. Weitere Informationen finden Sie unter *Bericht Full Disk Encryption Status auf Seite 4-16*.

Bericht Full Disk Encryption Status

In der folgenden Tabelle wird der Bericht **Full Disk Encryption Status** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-6. Beispiel für den Bericht Full Disk Encryption Status

HEADER	BEISPIEL	BESCHREIBUNG
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der Computername, der vom Endpoint Encryption Gerät verwendet wird.
Geräte-ID	1fabfbff-0001-06e5-000c-29 7085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
Anwendung	Full Disk Encryption	Der momentan installierte Endpoint Encryption Agent.
Status	Nicht verschlüsselt	Der aktuelle Status des Endpoint Encryption Geräts. Eine Liste der Verschlüsselungsstatuswerte finden Sie unter *Widget "Full Disk Encryption Status" auf Seite 4-15*.
Datum der letzten Synchronisierung	07.10.2013 11:05	Der Zeitpunkt, als die Richtlinien zum letzten Mal auf dem Endpoint Encryption Gerät von PolicyServer aktualisiert wurden.
Letzte Richtliniendurchsetzung	07.10.2013 11:05	Der Zeitpunkt, als Control Manager zum letzten Mal Richtlinienänderungen auf PolicyServer durchgesetzt hat.

Widget Erfolglose Anmeldeversuche am Endpoint Encryption Gerät

Auf dem Widget **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** werden alle Endpoint Encryption Geräte mit erfolglosen Anmeldeversuchen durch beliebige Benutzer (Endpoint Encryption Benutzer oder Nicht-Endpoint Encryption Benutzer) angezeigt. Erfolgloses Anmeldeversuche an einem Gerät stellen möglicherweise einen Sicherheitsverstoß dar oder der Endpoint Encryption Benutzer hat vielleicht seine Anmeldedaten vergessen.

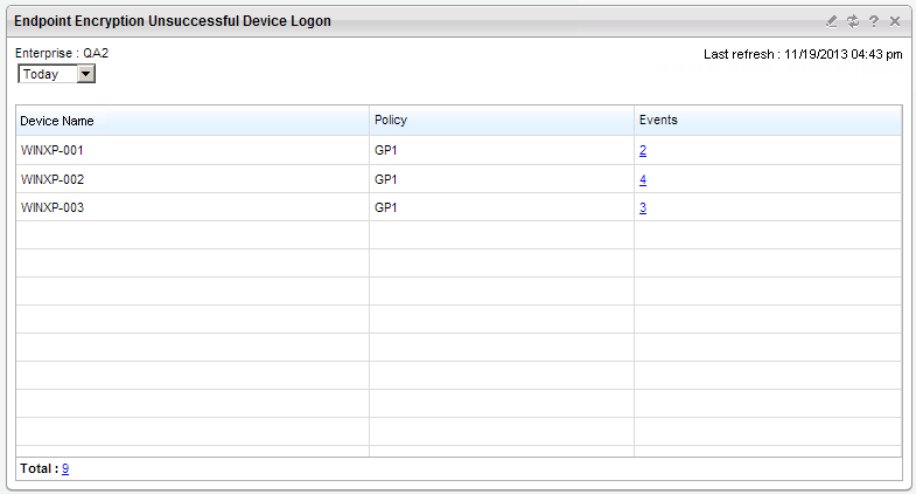


TABELLE 4-7. Beschreibung der Spalten des Widgets "Erfolglose Anmeldeversuche am Endpoint Encryption Gerät"

SPALTE	BESCHREIBUNG
Gerätename	Der Computername des Endpoint Encryption Geräts.
Richtlinie	Die Richtlinie, die das Endpoint Encryption Gerät verwaltet.

Spalte	Beschreibung
Ereignisse	Die Anzahl der Anmeldeversuche. Klicken Sie auf die Zahl, um den Bericht **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** anzuzeigen.

Bericht Erfolglose Anmeldeversuche am Endpoint Encryption Gerät

In der folgenden Tabelle wird der Bericht **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

Tabelle 4-8. Beispiel für den Bericht Erfolglose Anmeldeversuche am Endpoint Encryption Gerät

Header	Beispiel	Beschreibung
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der Computername, der vom Endpoint Encryption Gerät verwendet wird.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
IP-Adresse	10.1.152.219	Die IP-Adresse des Endpoint Encryption Geräts.
Anwendung	Full Disk Encryption	Der momentan installierte Endpoint Encryption Agent.

HEADER	BEISPIEL	BESCHREIBUNG
Anzeigename	Mary Jones	Der Vorname und der Nachname des Endpoint Encryption Benutzerkontos. Wenn es sich beim angegebenen Benutzernamen nicht um einen gültigen Endpoint Encryption Benutzernamen handelt, wird in der Spalte „Nicht aufgezeichnet“ angegeben.
Ereignis	Erfolglose Anmeldung per festem Kennwort	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Widget Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers

Auf dem Widget **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** werden alle Anmeldeversuche durch einen beliebigen Benutzer (Endpoint Encryption

Benutzer oder Nicht-Endpoint Encryption Benutzer) an einem beliebigen Endpoint Encryption Gerät angezeigt.

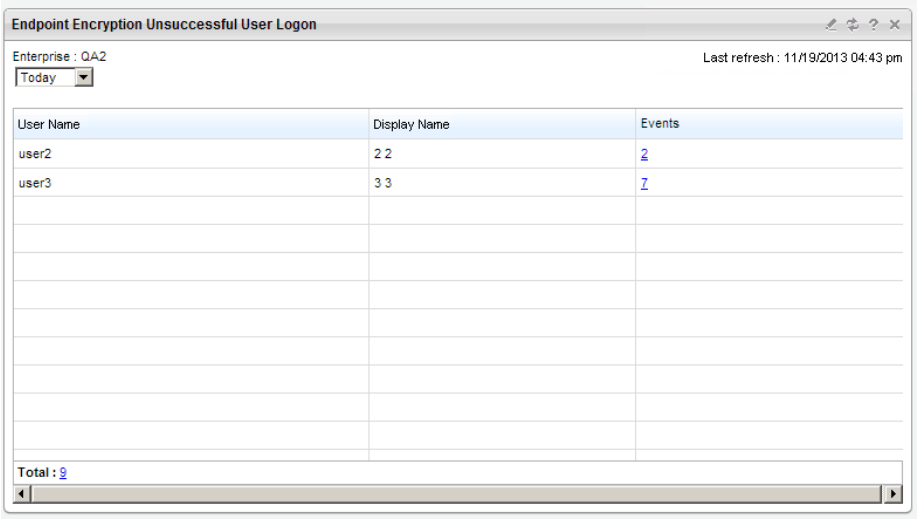


ABBILDUNG 4-5. Widget Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers

TABELLE 4-9. Beschreibung des Widgets Erfolglose Anmeldeversuche am Endpoint Encryption Gerät

SPALTE	BESCHREIBUNG
Benutzername	Der Name des Benutzers, der versuchte, sich an einem Endpoint Encryption Gerät anzumelden.
Anzeigename	Der Anzeigename des Benutzerkontos, das versuchte, sich am Endpoint Encryption Gerät anzumelden.
Ereignisse	Die Anzahl der Authentifizierungsversuche. Klicken Sie auf die Zahl, um den Bericht "Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers" anzuzeigen.

Bericht Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers

In der folgenden Tabelle wird der Bericht **Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-10. Beispiel für den Bericht Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der Computername, der vom Endpoint Encryption Gerät verwendet wird.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
IP-Adresse	10.1.152.219	Die IP-Adresse des Endpoint Encryption Geräts.
Anwendung	Full Disk Encryption	Der momentan installierte Endpoint Encryption Agent.
Anzeigename	Mary Jones	Der Vorname und der Nachname des Endpoint Encryption Benutzerkontos. Wenn es sich beim angegebenen Benutzernamen nicht um einen gültigen Endpoint Encryption Benutzernamen handelt, wird in der Spalte „Nicht aufgezeichnet“ angegeben.
Ereignis	Erfolglose Anmeldung per festem Kennwort	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Widget Endpoint Encryption Gerätesperrung

Das Widget **Endpoint Encryption Gerätesperrung** zeigt Endpoint Encryption Geräte an, die aufgrund von Richtlinieneinschränkungen gesperrt wurden.

Hinweis

Informationen zu Regeln zur Gerätesperrung von Endpoint Encryption finden Sie unter *Aktionen zum Sperren von Konten und Geräten auf Seite 3-26*.

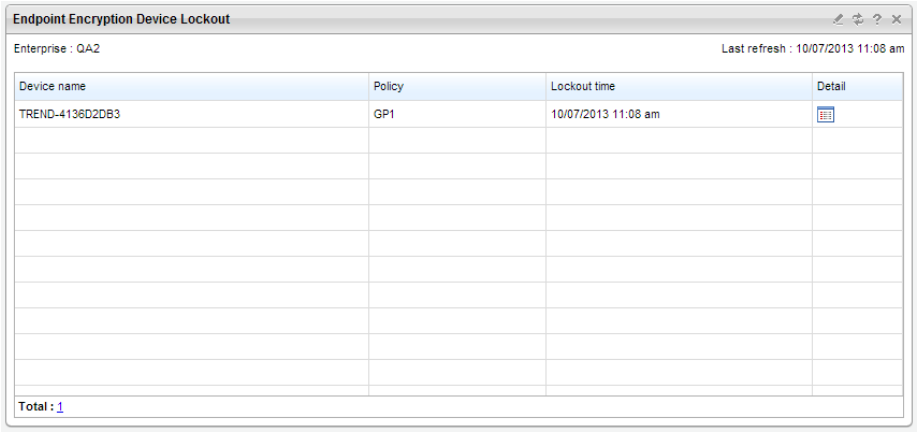


ABBILDUNG 4-6. Widget Endpoint Encryption Gerätesperrung

TABELLE 4-11. Beschreibung des Widgets Endpoint Encryption Gerätesperrung

HEADER	BESCHREIBUNG
Gerätename	Der Computername, der vom Endpoint Encryption Gerät verwendet wird.
Richtlinie	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.

Header	Beschreibung
Sperrung	Der Zeitpunkt, als PolicyServer den Befehl zum Sperren des Geräts gegeben hat. Das Endpoint Encryption Gerät wird faktisch erst gesperrt, nachdem der Endpoint Encryption Agent die Richtlinien mit PolicyServer synchronisiert hat.
Details	Klicken Sie auf das Detailsymbol, um den Bericht "Endpoint Encryption Gerätesperrung" anzuzeigen.

Klicken Sie unten im Widget auf die Zahl neben **Gesamt**, um den Bericht anzuzeigen.

Bericht Endpoint Encryption Gerätesperrung

In der folgenden Tabelle wird der Bericht **Endpoint Encryption Gerätesperrung** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

Hinweis

Informationen zu den Aktionen zum Sperren von Konten und Geräten finden Sie unter *Aktionen zum Sperren von Konten und Geräten auf Seite 3-26*.

Tabelle 4-12. Berichtsbeispiel für Endpoint Encryption Gerätesperrung

Header	Beispiel	Beschreibung
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie, die das Endpoint Encryption Gerät steuert.
Gerätename	TREND-4136D2DB3	Der Computername, der vom Endpoint Encryption Gerät verwendet wird.

HEADER	BEISPIEL	BESCHREIBUNG
Geräte-ID	1fabfbff-0001-06e5-000c-29 7085710000	Die eindeutige ID, die festgelegt wurde, nachdem der Endpoint Encryption Agent auf dem Endpunkt installiert und ein neues Endpoint Encryption Gerät bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpoint Encryption Geräts.
Anwendung	Full Disk Encryption	Der momentan installierte Endpoint Encryption Agent.
Anzeigename	Mary Jones	Der Vorname und der Nachname des Endpoint Encryption Benutzerkontos. Wenn es sich beim angegebenen Benutzernamen nicht um einen gültigen Endpoint Encryption Benutzernamen handelt, wird in der Spalte „Nicht aufgezeichnet“ angegeben.
Ereignis	Das Gerät wurde aufgrund einer Verletzung durch einen ungültigen Anmeldeversuch gesperrt.	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Widget Endpoint Encryption - Bericht zu Sicherheitsverstößen

Das Widget **Endpoint Encryption - Bericht zu Sicherheitsverstößen** zeigt die Sicherheitsverstöße aus folgenden Berichten an:

- **Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät**
- **Endpoint Encryption - Richtlinienmanipulation**
- **Endpoint Encryption - Protokollintegrität**

Beim Generieren eines Berichts werden alle Sicherheitsverstöße erfasst, die momentan von PolicyServer protokolliert wurden. Klicken Sie nach der Generierung auf die Zahl in der Spalte **Berichte**, um die generierten Berichte für diesen Verstoß anzuzeigen.

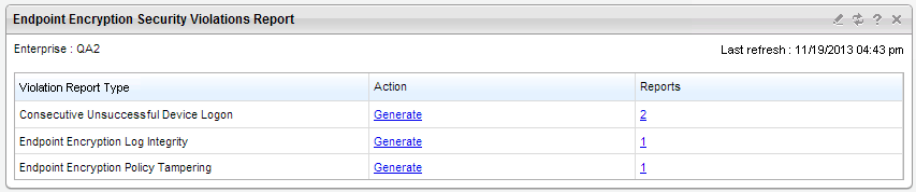


ABBILDUNG 4-7. Widget Endpoint Encryption - Bericht zu Sicherheitsverstößen

TABELLE 4-13. Beschreibung Endpoint Encryption - Bericht zu Sicherheitsverstößen

HEADER	BESCHREIBUNG
Typ des Berichts zu Verstößen	Die verfügbaren Berichttypen für verschiedene Verstöße.
Aktion	Klicken Sie auf **Generieren**, um einen neuen Bericht zu erstellen.
Berichte	Die Gesamtzahl der generierten Berichte für diesen Verstoß. Klicken Sie auf die Zahl, um die verfügbaren Berichte anzuzeigen.

Bericht Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät** beschrieben. Anhand der Informationen aus diesem Bericht sehen Sie, wann der Anmeldungsversuch

durchgeführt wurde, welches Endpoint Encryption Gerät betroffen ist und wie oft der Benutzer versucht hat, sich am Endpoint Encryption Gerät anzumelden.

TABELLE 4-14. Beispiel für den Bericht Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät

EINTRAG	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Gerätename	TREND-4136D2DB3	Der Computername, der vom Endpoint Encryption Gerät verwendet wird.
Versuche	5	Die Häufigkeit, wie oft ein Benutzer versuchte, sich am Endpoint Encryption Gerät anzumelden.

Endpoint Encryption - Bericht zu Richtlinienmanipulationen

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Bericht zu Richtlinienmanipulationen** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-15. Beispiel für Endpoint Encryption - Bericht zu Richtlinienmanipulationen

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Ereignis	Integritätsprüfung des Richtlinienwerts fehlgeschlagen	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Endpoint Encryption - Bericht zur Protokollintegrität

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Bericht zur Protokollintegrität** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 4-16. Beispiel für Endpoint Encryption - Bericht zur Protokollintegrität

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Die Uhrzeit, als das Ereignis aufgetreten ist.
Ereignis	Audit-Protokoll-Datensatz fehlt	Das protokollierte Ereignis einschließlich der Authentifizierungsmethode.

Kapitel 5

Richtlinien in Control Manager

In diesem Kapitel wird die Verwendung von Richtlinien erläutert. Weiterhin werden ausführliche Informationen zu einzelnen Richtlinienwerten bereitgestellt.

Es werden folgende Themen behandelt:

- *Gruppen auf Seite 5-2*
- *Richtlinien verstehen auf Seite 5-2*
- *Grundlegendes zu Richtlinientypen auf Seite 5-4*
- *Grundlegendes zu Einstellungen für das Richtlinienziel auf Seite 5-7*
- *Grundlegendes zur Liste der verwalteten Server auf Seite 5-31*
- *Richtlinienvorlagen aktualisieren auf Seite 5-36*

Gruppen

Um die Richtlinienverwaltung zu rationalisieren, führt Control Manager die PolicyServer MMC Gruppen- und Richtlinienhierarchie zusammen. Unabhängig von der von Ihnen bevorzugten Management-Konsole behält PolicyServer dieselbe Richtlinien- und Gruppenkonfiguration bei. Wenn Sie in Control Manager ein neues Richtlinienziel erstellen, zeigt PolicyServer MMC eine neue Gruppe an, die die Richtlinienkonfigurationen und die Benutzer enthält, die der Richtlinie hinzugefügt wurden.

Wichtig

Control Manager hat immer Vorrang. Alle mit PolicyServer MMC durchgeführten Änderungen an der Gruppenzuweisung werden beim nächsten Mal automatisch überschrieben, wenn Control Manager Richtlinien mit PolicyServer synchronisiert.

Richtlinien verstehen

Über die Richtlinienverwaltung können Administratoren die Produkteinstellungen auf verwalteten Produkten von einer einzelnen Management-Konsole aus durchsetzen. Administratoren erstellen eine Richtlinie, indem sie die Ziele auswählen und eine Liste der Produkteinstellungen konfigurieren.

Control Manager Richtlinien haben die folgenden Attribute:

TABELLE 5-1. Optionen für Control Manager Richtlinien

ATTRIBUT	BESCHREIBUNG
Name der Richtlinie	Der Name der Richtlinienkonfiguration.

ATTRIBUT	BESCHREIBUNG
Ziele	Administratoren können Ziele manuell auswählen oder Filter verwenden, um Zielen automatisch Richtlinien zuzuweisen. Die Methode zur Zielauswahl bestimmt den Richtlinientyp und wie die Richtlinie funktioniert. Weitere Informationen über Richtlinientypen finden Sie unter *Grundlegendes zu Richtlinientypen auf Seite 5-4*. Wenn Sie ein verwaltetes Produkt oder einen Endpunkt als Ziel einbeziehen möchten, vergewissern Sie sich, dass die Produktversion des verwalteten Produkts oder Endpunkts die Richtlinienverwaltung in Control Manager unterstützt. Das Fenster **Policy Template Settings** enthält Informationen zu den unterstützten Produktversionen.
Einstellungen	Nachdem Control Manager eine Richtlinie auf die Ziele verteilt hat, überschreiben die in der Richtlinie definierten Einstellungen die bestehenden Einstellungen in den Zielen. Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch. Obwohl lokale Administratoren Änderungen an den Einstellungen über die Konsole des verwalteten Produkts vornehmen können, werden die Änderungen jedes Mal überschrieben, wenn Control Manager die Richtlinieneinstellungen überschreibt. **Hinweis** Da Richtlinien nur alle 24 Stunden durchgesetzt werden, entsprechen die Produkteinstellungen in den Zielen möglicherweise nicht den Richtlinieneinstellungen, wenn lokale Administratoren Änderungen über die Konsole der verwalteten Produkte zwischen der Durchsetzungsperiode vornehmen.

Administratoren können im Fenster **Policy Management** die folgenden Aufgaben ausführen:

- *Eine Richtlinie erstellen auf Seite 3-12*
- *Eine Richtlinie bearbeiten auf Seite 5-29*
- *Eine Richtlinie löschen auf Seite 5-30*

- *Richtlinieneinstellungen kopieren auf Seite 5-28*

Hinweis

Verwenden Sie das **Produktverzeichnis**, um die verwaltete PolicyServer Instanz aus dem Ordner "Neues Element" in den Endpoint Encryption Ordner im Produktverzeichnis zu verschieben. Weitere Informationen finden Sie unter *Grundlegendes zum Produktverzeichnis auf Seite A-17*.

Grundlegendes zu Richtlinientypen

Control Manager unterstützt drei Richtlinientypen, die von Administratoren erstellt werden können. Jeder Richtlinientyp unterscheidet sich in der Auswahlmethode für Ziele, was sich auf die Arbeitsweise der Richtlinie auswirkt. Entsprechend der Beschreibung in der folgenden Tabelle werden die Richtlinientypen in der Richtlinienliste wie folgt sortiert.

TABELLE 5-2. Richtlinientypen

RICHTLINIENTYP	BESCHREIBUNG
Angebe	• Verwendet die Funktionen zum Durchsuchen und Suchen, um bestimmte Ziele zu finden und sie manuell einer Richtlinie zuzuweisen. • Nützlich, wenn Administratoren planen, bestimmte Einstellungen nur auf bestimmte Ziele zu verteilen. • Bleibt an statischer Position ganz oben in der Richtlinienliste und hat eine höhere Priorität als alle gefilterten Richtlinien.

RICHTLINIENTYP	BESCHREIBUNG
Gefiltert	• Verwendet einen Filter, um automatisch aktuelle und zukünftige Ziele der Richtlinie zuzuweisen. • Nützlich, um Standardeinstellungen an eine Gruppe von Zielen zu verteilen. • Administratoren können die Priorität von gefilterten Richtlinien in der Richtlinienliste ändern. • Weitere Informationen darüber, wie Control Manager Ziele den gefilterten Richtlinien zuweist, finden Sie unter *Endpunkte gefilterten Richtlinien zuweisen auf Seite 5-5*. **Hinweis** • Wenn ein Administrator die Richtlinienliste neu ordnet, führt Control Manager eine Neuzuweisung der Ziele an verschiedene gefilterte Richtlinien auf Grundlage der Zielkriterien und der Benutzerrollen des jeweiligen Verfassers der Richtlinie durch. • Gefilterte Richtlinien sind nur zur Verwaltung von OfficeScan Einstellungen verfügbar.
Entwurf	Ermöglicht, dass Administratoren die Richtlinieneinstellungen als Entwurf ohne Auswahl von Zielen speichern können. Control Manager speichert Entwurfsrichtlinien mit der untersten Priorität ganz unten in der Liste.

Endpunkte gefilterten Richtlinien zuweisen

Wenn ein neuer Endpunkt in Control Manager registriert wird, wird die Liste der gefilterten Richtlinien in absteigender Reihenfolge abgearbeitet. Control Manager weist den neuen Endpunkt einer gefilterten Richtlinie zu, wenn die folgenden Bedingungen erfüllt sind:

- Der neue Endpunkt stimmt mit dem Zielkriterium in der Richtlinie überein
- Der Verfasser der Richtlinie verfügt über die Berechtigung, den neuen Endpunkt zu verwalten

Dieselbe Aktion gilt für einen Endpunkt, der bereits einer Richtlinie zugewiesen wurde, wobei diese jedoch später vom Verfasser der Richtlinie gelöscht wurde.

Hinweis

Bei Endpunkten, die gerade in Control Manager registriert wurden, und solchen, die gerade aus gelöschten Richtlinien freigegeben wurden, gibt es eine dreiminütige Übergangsfrist, während der keine Endpunkte zugewiesen werden. Während dieser Periode haben die Endpunkte vorübergehend keine Richtlinien.

Wenn ein Endpunkt die Zielkriterien von keiner gefilterten Richtlinien erfüllt, wird der Endpunkt keiner Richtlinie zugeordnet. Control Manager weist diese Endpunkte erneut zu, wenn die folgenden Aktionen eintreten:

- Eine neue gefilterte Richtlinie wird erstellt
- Eine gefilterte Richtlinie wird bearbeitet
- Gefilterte Richtlinien werden neu geordnet
- Täglicher Zuweisungszeitplan für Endpunkte

  Control Manager verwendet einen täglichen Zuweisungszeitplan für Endpunkte, um sicherzustellen, dass Endpunkte den richtigen Richtlinien zugewiesen werden. Diese Aktion finden einmal pro Tag um 15:15 Uhr statt. Wenn sich die Eigenschaften eines Endpunkts ändern, z. B. das Betriebssystem oder die IP-Adresse, müssen diese Endpunkte mit Hilfe des täglichen Zeitplans den richtigen Richtlinien neu zugewiesen werden.

  Hinweis

  Wenn die Endpunkte offline sind, während der tägliche Zuweisungszeitplan für Endpunkte ausgeführt wird, wird der Richtlinienstatus für diese Endpunkte nicht geändert (ausstehend), bis sie online gehen.

Wenn die oben beschriebenen Aktionen ausgeführt werden, ordnet Control Manager die Endpunkte auf Grundlage der folgenden Bedingungen zu:

TABELLE 5-3. Endpunktzuordnung für gefilterte Richtlinien

	Neue Endpunkte oder Endpunkte aus gelöschten Richtlinien	Endpunkte ohne Richtlinien	Endpunkte mit Richtlinien
Eine neue Richtlinie erstellen		●	
Eine Richtlinie bearbeiten	●	●	●
Gefilterte Richtlinien werden neu geordnet	●	●	●
Täglicher Zuweisungszeitplan für Endpunkte	●	●	●

Grundlegendes zu Einstellungen für das Richtlinienziel

In diesem Abschnitt wird erläutert, wie verschiedene Fenster zum Ändern einer Richtlinie verwendet werden können. Das Verfahren zum Ändern aller Richtlinien wird hier jedoch nicht erläutert. Alle Richtlinien haben Standardwerte. Der PolicyServer MMC verfügt über mehrere allgemeine Fenster zum Ändern von Richtlinien. Die eine Richtlinie weist ein Editorfenster auf, in dem mit der Richtlinie verbundene Zahlen, Bereiche und Werte geändert werden können, während eine andere Richtlinie über ein Fenster zum Ändern von Textzeichenfolgen verfügt.

Beachten Sie beim Verwalten von Richtlinien Folgendes:

- Richtlinien können nach Anwendung in jeder Gruppe konfiguriert werden.
- Richtlinienvererbung findet nur statt, wenn eine Untergruppe erstellt wird. Weitere Informationen zu Gruppenberechtigungen finden Sie unter *Info über Gruppen auf Seite 10-2*.

Grundlegendes zur Richtlinienliste

In der Richtlinienliste werden die Informationen und der Status der Richtlinien angezeigt, die von allen Benutzern erstellt wurden. Wenn ein neuer Endpunkt in Control Manager registriert wird, wird die Liste der gefilterten Richtlinien in absteigender Reihenfolge abgearbeitet. Control Manager weist den neuen Endpunkt einer gefilterten Richtlinie zu, wenn die folgenden Bedingungen erfüllt sind:

- Der neue Endpunkt stimmt mit dem Zielkriterium der Richtlinie überein
- Der Verfasser der Richtlinie verfügt über die Berechtigung, den neuen Endpunkt zu verwalten

Die folgende Tabelle beschreibt die Elemente in der Richtlinienliste.

TABELLE 5-4. Richtlinienliste

MENÜELEMENT	BESCHREIBUNG
Priorität	Zeigt die Priorität der Richtlinien an. • Control Manager zeigt eine Liste der Richtlinien an, die von der höchsten zur niedrigsten Priorität geordnet ist. • When Administratoren eine gefilterte Richtlinie erstellen, speichert Control Manager die neue Richtlinie als niedrigste Priorität. • Eine angegebene Richtlinie hat eine höhere Priorität als jede gefilterte Richtlinie und bleibt in der Liste ganz oben. Administratoren können angegebene Richtlinien nicht neu sortieren. • Control Manager platziert Entwurfsrichtlinien ganz unten in der Liste.
Richtlinie	Zeigt den Namen der Richtlinie an.

MENÜELEMENT	BESCHREIBUNG
Ziele	Zeigt an, wie Administratoren Ziele für die Richtlinie auswählen. • Angabe: Wählt mit Hilfe der Funktionen zum Durchsuchen und Suchen bestimmte Ziele für die Richtlinie. Angegebene Richtlinien bleiben statisch ganz oben in der Richtlinienliste und haben eine höhere Priorität als jede gefilterte Richtlinie. • Gefiltert: Verwendet einen Filter, um automatisch aktuelle und zukünftige Endpunkte der Richtlinie zuzuweisen. Administratoren können die Priorität der gefilterten Richtlinien neu organisieren. • Keine: Der Verfasser der Richtlinie speichert die Richtlinie als Entwurf, ohne Ziele auszuwählen.
Verteilt	Zeigt die Anzahl der Ziele an, die die Richtlinieneinstellungen angewendet haben.
Ausstehend	Zeigt die Anzahl der Ziele an, die die Richtlinieneinstellungen nicht angewendet haben. Klicken Sie auf die Zahl für "Ausstehend", um den Status der Richtlinie zu überprüfen.
Verfasser	Zeigt den Benutzer an, der die Richtlinie erstellt hat.
Endpunkte/Produkte ohne Richtlinien	Zeigt die Anzahl der verwalteten Produkte oder Endpunkte an, denen Control Manager keine Richtlinie zugewiesen hat.
Gesamtzahl der Endpunkte/Produkte	Zeigt die Anzahl der verwalteten Produkte oder Endpunkte an, die für die Richtlinienverwaltung verfügbar sind.

Hinweis

In den Werten in "Verteilt", "Ausstehend", "Endpunkte/Produkte ohne Richtlinien" und "Gesamtzahl der Endpunkte/Produkte" werden nur die Endpunkte oder verwalteten Produkte erfasst, die ein Administrator laut seinen Berechtigungen verwalten darf.

Eine Richtlinie erstellen

Das folgende Verfahren erklärt, wie Sie eine Control Manager Richtlinie konfigurieren, die sich auf Endpoint Encryption Benutzer und Geräte auswirkt.

Wichtig

Wenn Sie ein Benutzerkonto der Richtlinie hinzufügen möchten, vergewissern Sie sich, dass das Benutzerkonto bereits vorhanden ist.

Hinweis

Informationen zu den verfügbaren Richtlinieneinstellungen finden Sie unter *Endpoint Encryption Richtlinieneinstellungen auf Seite 5-14*.

Weitere Informationen zum Hinzufügen von Endpoint Encryption Benutzern finden Sie unter *Benutzer zu Endpoint Encryption hinzufügen auf Seite 6-4*.

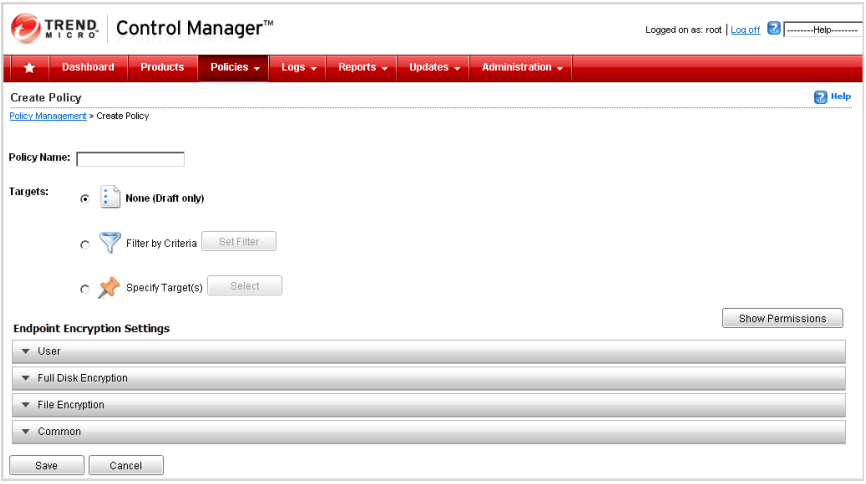
Informationen zur Konfiguration von Active Directory finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Informationen zur Richtlinienzuordnung zwischen Control Manager und PolicyServer MMC finden Sie unter *Richtlinienzuordnung zwischen Management-Konsolen auf Seite D-1*.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.
2. Wählen Sie im Listenfeld **Produkt** die Option **Endpoint Encryption**.
3. Klicken Sie auf **Erstellen**.

   Das Fenster **Richtlinie erstellen** wird angezeigt.



4. Geben Sie einen Richtliniennamen an.

5. Aktivieren Sie eine der folgenden Optionen für das Richtlinienziel:

   - **Keines (nur Entwurf)**: Sie erstellen eine Richtlinie ohne Ziele (Endpunkte).
   - **Filter nach Kriterien**: Endpoint Encryption unterstützt keine Filterung nach Kriterien.
   - **Ziel(e) angeben**: Sie geben vorhandene Endpunkte an.

   Hinweis

   Weitere Informationen über Richtlinienziele finden Sie unter *Richtlinienziele angeben auf Seite 3-14*.

6. Sie können die Richtlinieneinstellungen für Endpoint Encryption angeben.

   - Konfigurieren Sie **Benutzerrichtlinien**.

     Weitere Informationen finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

   - Konfigurieren Sie die Richtlinien für **Full Disk Encryption**.

Weitere Informationen finden Sie unter *Full Disk Encryption Regeln konfigurieren auf Seite 3-18*.

- Konfigurieren Sie die Richtlinien für **File Encryption**.

  Weitere Informationen finden Sie unter *File Encryption Regeln konfigurieren auf Seite 3-20*.

- Konfigurieren Sie die **allgemeinen Richtlinien**.

  Weitere Informationen finden Sie unter *Allgemeine Regeln für Richtlinien konfigurieren auf Seite 3-23*.

7. Klicken Sie auf **Speichern**.

Richtlinienziele angeben

Im Fenster **Ziel(e) angeben** weisen Sie die Endpoint Encryption Geräte der Richtlinie zu.

Hinweis

Das Fenster **Ziel(e) angeben** wird angezeigt, wenn Sie eine neue Richtlinie erstellen. Informationen zum Erstellen einer Richtlinie finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

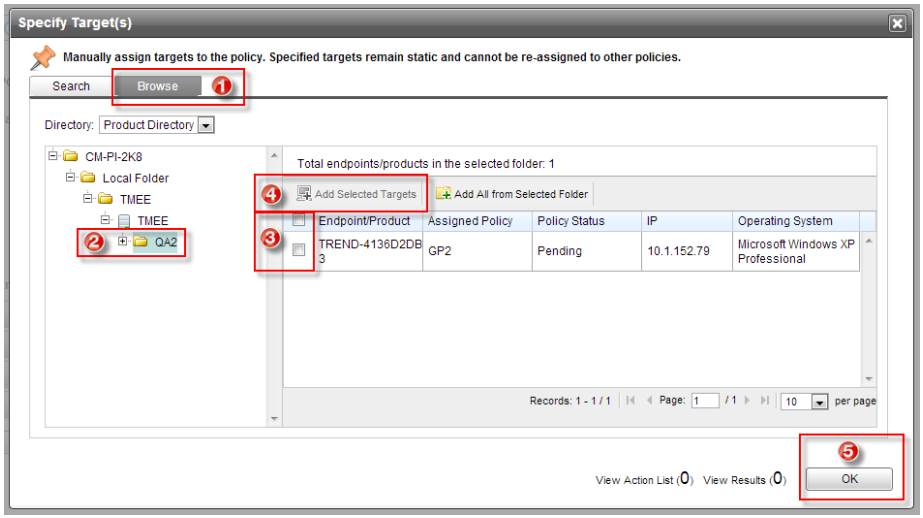


ABBILDUNG 5-1. Richtlinienziele angeben

Prozedur

1. Klicken Sie im Fenster **Ziel(e) angeben** auf die Registerkarte **Durchsuchen**.
2. Erweitern Sie die Struktur im linken Fensterbereich, um den verwalteten Ordner zu wählen.

   Beispiel: **CM-PI-2K8 > Lokaler Ordner > TMEE > TMEE > QA2**
3. Wählen Sie die entsprechenden Endpoint Encryption Geräte, oder aktivieren Sie das obere Kontrollkästchen, um alle Endpoint Encryption Geräte auszuwählen, die auf der aktuellen Seite aufgelistet werden.
4. Klicken Sie auf **Ausgewählte Ziele hinzufügen**.

Hinweis

Wenn Sie sofort alle Geräte im verwalteten Ordner auswählen möchten, klicken Sie auf **Alle aus ausgewähltem Ordner hinzufügen**.

„Aktionsliste anzeigen“ und „Ergebnisse anzeigen“ werden basierend auf der Auswahl aktualisiert.

5. Klicken Sie auf **OK**.

Endpoint Encryption Richtlinieneinstellungen

Regeln für Endpoint Encryption Benutzer konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die die Authentifizierung und Endpoint Encryption Benutzerkonten betreffen.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf **Benutzer**.

Das Fenster zu den Richtlinienregeleinstellungen **Benutzer** wird angezeigt.

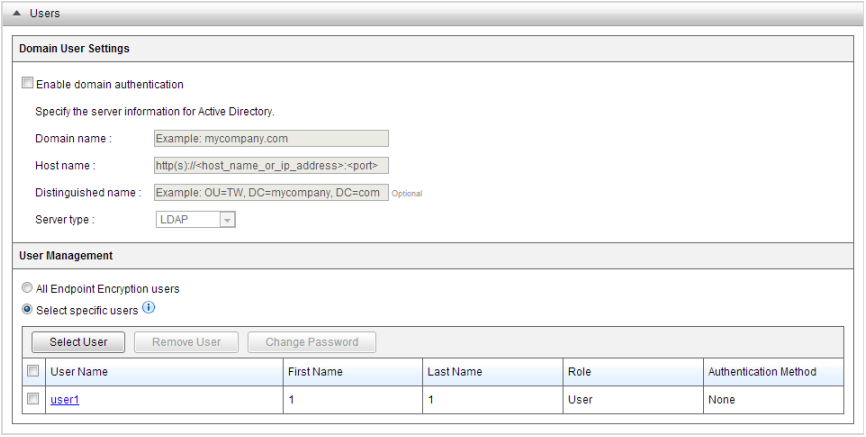


ABBILDUNG 5-2. Richtlinienregeln für Endpoint Encryption Benutzer

3. Wählen Sie unter **Domänenbenutzereinstellungen** die Option **Domänenauthentifizierung aktivieren**, um festzulegen, ob die Domänenauthentifizierung für Benutzer erforderlich ist.

Wichtig

Die Active Directory (AD) Synchronisierung erfordert, dass PolicyServer drei aktivierte Komponenten hat:

a. Konfigurieren Sie die AD-Domäne.

b. Lonfigurieren Sie die Richtliniengruppe, um auf die entsprechende Organisationseinheit (OU) zu verweisen.

c. Konfigurieren Sie die Richtliniengruppe mit entsprechenden Anmeldedaten für den Zugriff auf die AD-Domäne, die dem „Eindeutigen Namen“ der Richtliniengruppe entspricht.

Informationen zur Konfiguration der Domänenauthentifizierung finden Sie unter *PolicyServer - Active Directory-Synchronisierung* im *Endpoint Encryption Installations- und Migrationshandbuch*.

---

4. Konfigurieren Sie unter **Benutzerverwaltung** den Benutzerzugriff.

- Wählen Sie **Alle Benutzer von Endpoint Encryption**, um allen Benutzern, Domänen und lokalen Konten zu erlauben, Endpoint Encryption Geräte zu authentifizieren.
- Wählen Sie **Bestimmte Benutzer auswählen**, um festzulegen, welche bereits hinzugefügten Endpoint Encryption Benutzer sich an verwalteten Endpunkten authentifizieren können.

Hinweis

Richtlinienregeln wirken sich nur auf vorhandene Benutzerkonten aus. Vor der Konfiguration von Richtlinien können Sie neue Benutzer mit dem Widget "Endpoint Encryption Benutzer" hinzufügen. Weitere Informationen finden Sie unter *Benutzer zu Endpoint Encryption hinzufügen auf Seite 6-4*.

Full Disk Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf Full Disk Encryption Geräte auswirken.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf **Full Disk Encryption**.

Das Fenster mit den Einstellungen für **Full Disk Encryption** Richtlinienregeln wird angezeigt.

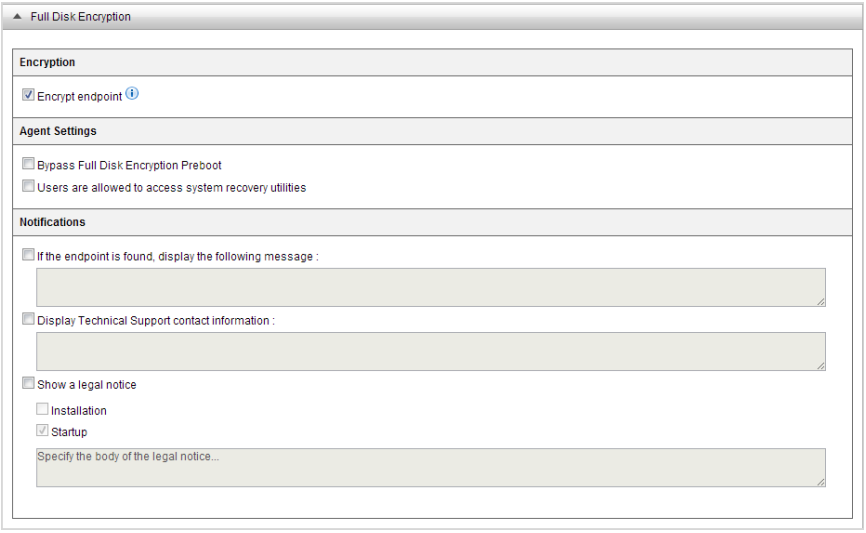


ABBILDUNG 5-3. Full Disk Encryption Richtlinienregeln

3. Wählen Sie unter **Verschlüsselung** die Option **Gerät verschlüsseln**, um eine Festplattenverschlüsselung zu starten, wenn der Endpoint Encryption Agent Richtlinien mit PolicyServer synchronisiert.

Warnung!

Sie sollten Full Disk Encryption Agents nicht verschlüsseln, ohne zuvor die Festplatte des Endpunkts vorzubereiten.

Informationen zur Vorbereitung der Festplatte finden Sie unter *Full Disk Encryption - Überblick über die Verteilung* im *Endpoint Encryption Installationshandbuch*.

4. Wählen Sie unter **Agent-Einstellungen** die folgenden Optionen:

   - Wählen Sie **Full Disk Encryption Preboot umgehen**, um dem Benutzer die Berechtigung zu geben, sich direkt bei Windows ohne den Schutz der Preboot-Authentifizierung zu authentifizieren.

- Wählen Sie **Benutzer sind berechtigt, auf die Systemwiederherstellungstools des Geräts zuzugreifen**, um Benutzern zu erlauben, auf die Wiederherstellungskonsole zuzugreifen.

  Informationen zu den konfigurierbaren Optionen und verfügbaren Tools in Full Disk Encryption finden Sie unter *Full Disk Encryption – Wiederherstellungskonsole auf Seite 14-21*.

5. Konfigurieren Sie die folgenden Optionen unter **Benachrichtigungen**:

   - Wählen Sie **Falls der Endpunkt gefunden wird, folgende Meldung anzeigen**, um eine Meldung anzuzeigen, wenn die Richtlinie **Falls gefunden** aktiv ist.
   - Wählen Sie **Kontaktdaten für den Technischen Support anzeigen**, um eine Meldung anzuzeigen, wenn sich der Benutzer am Full Disk Encryption Agent anmeldet.
   - Wählen Sie **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von Full Disk Encryption Agent anzuzeigen.

File Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf File Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf "File Encryption".

Das Fenster mit den Einstellungen für **File Encryption** Richtlinienregeln wird angezeigt.

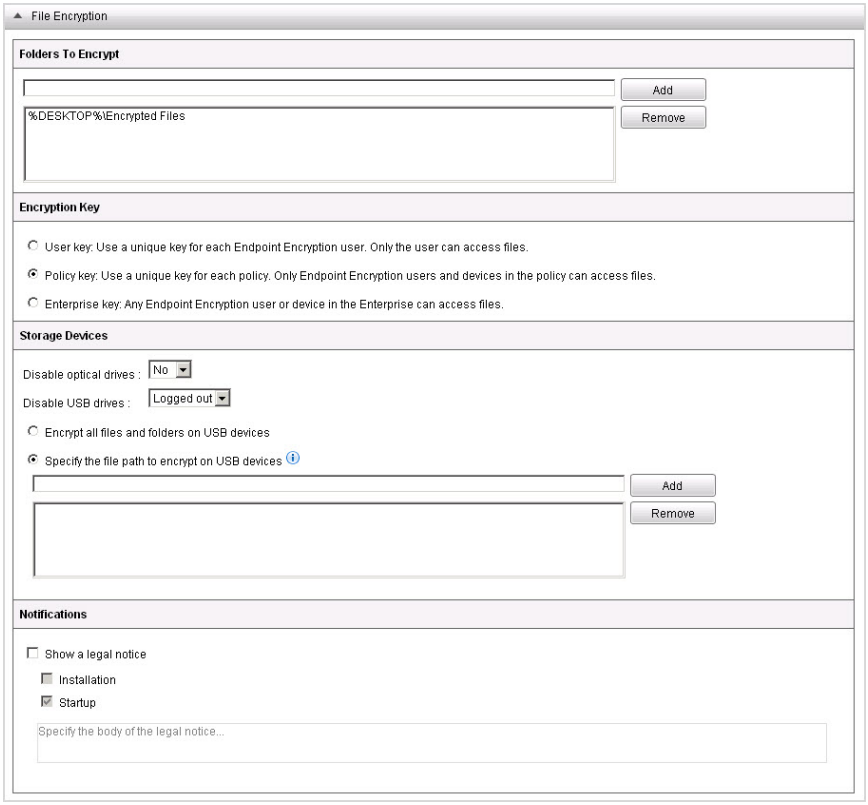

File Encryption
Folders To Encrypt
Add
%DESKTOP%\Encrypted Files
Remove
Encryption Key
User key: Use a unique key for each Endpoint Encryption user. Only the user can access files.
Policy key: Use a unique key for each policy. Only Endpoint Encryption users and devices in the policy can access files.
Enterprise key: Any Endpoint Encryption user or device in the Enterprise can access files.
Storage Devices
Disable optical drives :
No
Disable USB drives :
Logged out
Encrypt all files and folders on USB devices
Specify the file path to encrypt on USB devices
Add
Remove
Notifications
Show a legal notice
Installation
Startup
Specify the body of the legal notice...

ABBILDUNG 5-4. File Encryption Richtlinienregeln

3. Legen Sie unter **Zu verschlüsselnde Ordner** die Ordner fest, die auf dem Endpunkt automatisch erstellt und verschlüsselt werden, wenn der File Encryption Agent Richtlinien synchronisiert.

4. Wählen Sie unter **Verschlüsselungsschlüssel** die Verschlüsselung für den verschlüsselten File Encryption Ordner.

- **Benutzerschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jeden Endpoint Encryption Benutzer. Nur der Endpoint Encryption Benutzer kann Dateien entschlüsseln, die von ihm oder von ihr verschlüsselt wurden.
- **Richtlinienschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jede Richtlinie. Nur Endpoint Encryption Benutzer und Geräte in der Richtlinie können Dateien entschlüsseln.
- **Unternehmensschlüssel**: Alle Endpoint Encryption Benutzer oder Geräte im Unternehmen können Dateien entschlüsseln.

Hinweis

Durch die Auswahl von **Richtlinienschlüssel** oder **Unternehmensschlüssel** steuern Sie den Austausch des gemeinsamen Schlüssels für File Encryption. Weitere Informationen finden Sie unter *File Encryption Verschlüsselung mit gemeinsamem Schlüssel auf Seite 13-17*.

5. Konfigurieren Sie die folgenden Optionen unter **Speichergeräte**:
   - Wählen Sie **Optisches Laufwerk deaktivieren**, um festzulegen, ob der Zugriff auf Wechselmedien vom Endpunkt aus möglich ist.
   - Wählen Sie **USB-Laufwerk deaktivieren**, um festzulegen, ob USB-Ports deaktiviert sind. Folgende Optionen sind möglich:
     - **Immer**
     - **Abgemeldet**
     - **Nie**
   - Wählen Sie **Alle Dateien und Ordner auf USB-Geräten verschlüsseln**, um automatisch alle Dateien und Ordner auf Wechselmedien zu verschlüsseln, wenn diese mit dem Endpunkt verbunden sind.
   - Wählen Sie **Zu verschlüsselnden Dateipfad auf USB-Geräten angeben**, um verschlüsselte Ordner auf USB-Laufwerken hinzuzufügen oder zu entfernen. Nicht vorhandene Ordner werden erstellt. Wenn kein Laufwerksbuchstabe angegeben wird, gilt diese Regel für alle USB-Geräte.

6. Wählen Sie unter **Benachrichtigungen** die Option **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von File Encryption Agent anzuzeigen.

Allgemeine Regeln für Richtlinien konfigurieren

In diesem Abschnitt werden die konfigurierbaren Optionen für Richtlinienregeln erläutert, die sich auf alle Endpoint Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.

   Weitere Informationen finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

2. Klicken Sie auf **Allgemein**.

Das Fenster zu den Richtlinienregeleinstellungen **Allgemein** wird angezeigt.

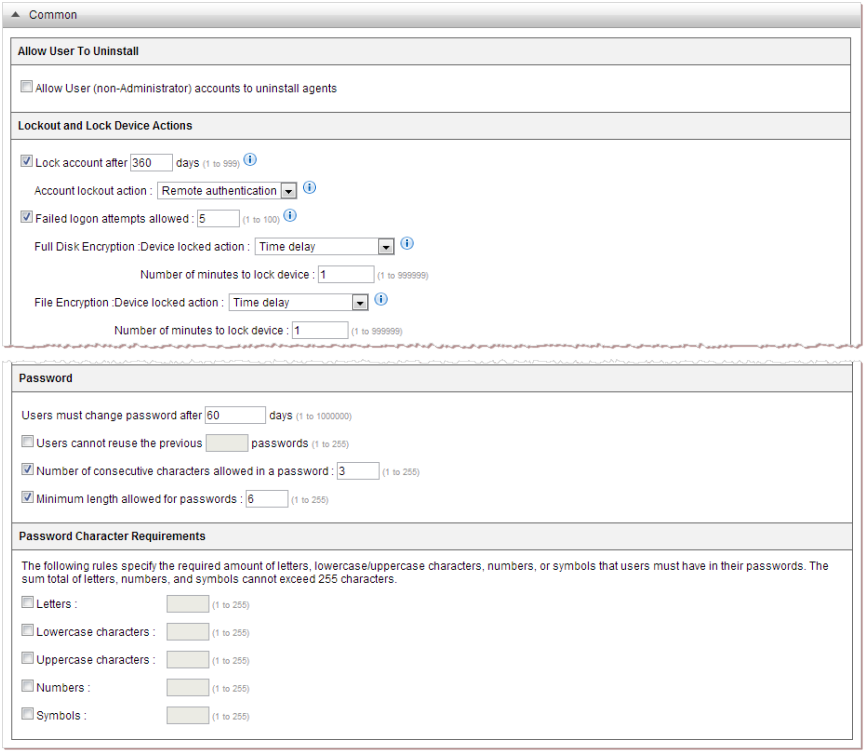

Common
Allow User To Uninstall
Allow User (non-Administrator) accounts to uninstall agents
Lockout and Lock Device Actions
Lock account after 360 days (1 to 999)
Account lockout action : Remote authentication
Failed logon attempts allowed : 5 (1 to 100)
Full Disk Encryption :Device locked action : Time delay
Number of minutes to lock device : 1 (1 to 999999)
File Encryption :Device locked action : Time delay
Number of minutes to lock device : 1 (1 to 999999)
Password
Users must change password after 60 days (1 to 1000000)
Users cannot reuse the previous passwords (1 to 255)
Number of consecutive characters allowed in a password : 3 (1 to 255)
Minimum length allowed for passwords : 6 (1 to 255)
Password Character Requirements
The following rules specify the required amount of letters, lowercase/uppercase characters, numbers, or symbols that users must have in their passwords. The sum total of letters, numbers, and symbols cannot exceed 255 characters.
Letters : (1 to 255)
Lowercase characters : (1 to 255)
Uppercase characters : (1 to 255)
Numbers : (1 to 255)
Symbols : (1 to 255)

ABBILDUNG 5-5. Allgemeine Richtlinienregeln

3. Wählen Sie unter **Deinstallation durch Benutzer zulassen** die Option **Nicht-Administratorkonten können die Agent-Software deinstallieren**, um allen Endpoint Encryption Benutzern zu erlauben, den Agent zu deinstallieren.

Hinweis

Standardmäßig können nur Unternehmensadministratoren Endpoint Encryption Agents deinstallieren.

4. Konfigurieren Sie unter **Aktionen zum Sperren von Geräten** die folgenden Optionen:

- Wählen Sie **Konto sperren nach <Anzahl> Tage**, um die Anzahl der Tage anzugeben, nach denen das Endpoint Encryption Gerät gesperrt wird, wenn die Richtlinien nicht synchronisiert werden.

  - Geben Sie mit **Kontosperraktion** an, ob bei einer Sperrung die Remote-Authentifizierung oder Löschung aktiviert werden soll.

    Hinweis

    Weitere Informationen zu den Sperroptionen finden Sie unter *Aktionen zum Sperren von Konten und Geräten auf Seite 3-26*.

- Wählen Sie **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**, um anzugeben, wie viele Authentifizierungsversuche möglich sind, bevor das Endpoint Encryption Gerät gesperrt wird.

- Konfigurieren Sie für Full Disk Encryption oder File Encryption Geräte Folgendes separat:

  - Geben Sie mit **Aktion zur Gerätesperrung** an, ob bei einer Sperrung die „Remote-Authentifizierung“ oder die „Löschung“ aktiviert werden soll.

    Hinweis

    Weitere Informationen zu den Sperroptionen finden Sie unter *Aktionen zum Sperren von Konten und Geräten auf Seite 3-26*.

  - Geben Sie unter **Anzahl der Minuten, die das Gerät gesperrt wird** die Dauer der Zeitverzögerung an, die das Endpoint Encryption Gerät gesperrt ist und nicht authentifiziert werden kann.

5. Konfigurieren Sie unter **Kennwort** die folgenden Optionen:

   - Wählen Sie **Benutzer muss das Kennwort nach <Anzahl> Tagen ändern**, um anzugeben, wenn ein Benutzer aufgefordert wird, das Kennwort zu aktualisieren.

   - Wählen Sie **Benutzer darf die vorherigen <Anzahl> Kennwörter nicht wiederverwenden**, um anzugeben, wie viele vorherige Kennwörter der Benutzer nicht verwenden darf.

- Wählen Sie **Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort**, um anzugeben, wie viele gleiche Zeichen ein Kennwort enthalten darf.
- Wählen Sie **Zulässige Mindestlänge für Kennwörter**, um anzugeben, aus wie vielen Zeichen ein Kennwort mindestens bestehen muss.

6. Legen Sie unter **Kennwortvoraussetzungen** die Einschränkungen in Bezug auf Zeichen in Kennwörtern fest.
   - **Buchstaben**
   - **Kleinbuchstaben**
   - **Großbuchstaben**
   - **Zahlen**
   - **Symbole**

Wichtig

Die Gesamtzahl der Buchstaben, Ziffern und Symbole kann höchstens 255 betragen.

Aktionen zum Sperren von Konten und Geräten

Einige Richtlinien verfügen über Einstellungen zum Sperren eines Benutzerkontos oder eines Geräts auf Grundlage bestimmter Kriterien. Aktionen zur Konto- oder Gerätesperrung wirken sich auf das Endpoint Encryption Gerät aus, unabhängig davon, ob der Agent die Richtlinien mit PolicyServer synchronisiert. Wenn ein Agent beispielsweise für eine bestimmte Zeitdauer nicht mit PolicyServer kommuniziert, sperrt der Endpoint Encryption Agent automatisch das Endpoint Encryption Gerät. Die nachfolgende Tabelle vermittelt Ihnen ein Verständnis der verfügbaren Aktionen zur Sperrung von Konten und Geräten.

TABELLE 5-5. Kontosperraktionen

AKTION	BESCHREIBUNG
Remote-Authentifizierung	Benutzer können sich so lange nicht am Endpoint Encryption Gerät anmelden, bis der Technische Support Unterstützung zur Remote-Authentifizierung bereitstellt.
Löschen	Wenn der Agent das nächste Mal die Richtlinien synchronisiert, werden alle Daten gelöscht.

Hinweis

Kontosperraktionen werden wirksam, wenn der Endpoint Encryption Agent innerhalb eines bestimmten Zeitraums (der durch die Richtlinie festgelegt wird) nicht mit PolicyServer kommuniziert.

TABELLE 5-6. Gerätesperraktionen

AKTION	BESCHREIBUNG
Löschen	Wenn der Endpoint Encryption Agent das nächste Mal die Richtlinien synchronisiert, werden alle Daten gelöscht.
Remote-Authentifizierung	Benutzer können sich so lange nicht an den Endpoint Encryption Geräten anmelden, bis der Technische Support Unterstützung zur Remote-Authentifizierung bereitstellt.
Zeitverzögerung	Benutzer können sich für eine bestimmte Zeitdauer nicht an den Endpoint Encryption Geräten anmelden.

Hinweis

Gerätesperraktionen werden wirksam, wenn der Endpoint Encryption Benutzer zu häufig erfolglos versucht hat, sich am Endpoint Encryption Gerät anzumelden (die Häufigkeit wird in der Richtlinie festgelegt).

Richtlinienregeln für die Remote-Hilfe

In der folgenden Tabelle werden die Speicherorte der Richtlinien für die Konten- und Gerätesperrung beschrieben, die sich auf die Remote-Hilfe-Authentifizierung auswirken.

Diese Informationen vermitteln ein Verständnis dafür, welche Richtlinien festgelegt werden sollten.

TABELLE 5-7. Richtlinienspeicherorte für die Remote-Hilfe

NAME DER RICHTLINIE	MENÜPFAD FÜR POLICYSERVER MMC	MENÜPFAD FÜR CONTROL MANAGER	BESCHREIBUNG
Kontosperraktion	**Anmelden** > **Kontosperraktion**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Kontosperraktion**	Die Maßnahme, die durchgeführt wird, nachdem die Zeitdauer in „Kontosperraktionen “ abgelaufen ist. Mögliche Maßnahmen sind: Löschen, Remote-Authentifizierung
Zeitraum bis Kontosperrung	**Anmelden** > **Zeitraum bis Kontosperrung**	**Allgemein** > **Aktionen zum Sperren von Geräten** > **Konto sperren nach [ ] Tagen**	Die Anzahl von Tagen, die ein Gerät ohne Kommunikation mit PolicyServer sein kann, bevor die „Kontosperraktion“ ausgeführt wird.
Aktion zur Gerätesperrung	Für jeden Agent: **Anmelden** > **Aktion zur Gerätesperrung**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Aktion zur Gerätesperrung**	Die Aktion, die durchgeführt wird, wenn der in der Richtlinie „Zulässige Anzahl fehlgeschlagener Anmeldeversuche“ festgelegte Wert überschritten wurde. Unterstütze Maßnahmen: Zeitverzögerung, Löschen, Remote-Authentifizierung

Name der Richtlinie	Menüpfad für PolicyServer MMC	Menüpfad für Control Manager	Beschreibung
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Für jeden Agent: **Anmelden** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Für jeden Agent: **Allgemein** > **Aktionen zum Sperren von Geräten** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche, bevor die Aktion zur „Gerätesperrung“ ausgeführt wird.

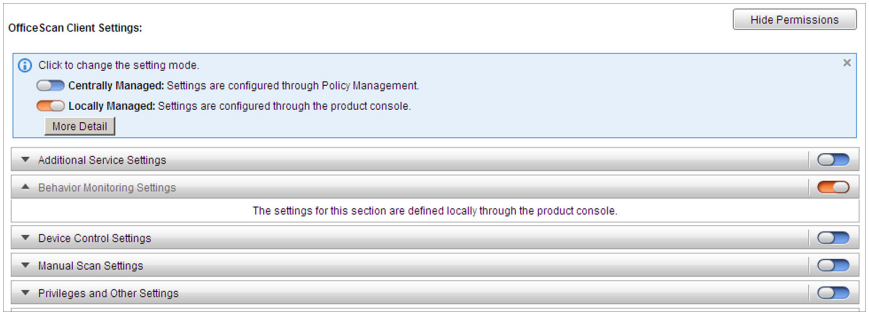
Einstellungsberechtigungen ändern

Bei der Konfiguration von Richtlinieneinstellungen können Administratoren den Administratoren für verwaltete Produkte die Berechtigung zuweisen, die Einstellungen von bestimmten Funktionen zu definieren. Führen Sie die folgenden Schritte aus, um die Einstellungsberechtigungen beim Erstellen oder Bearbeiten einer Richtlinie zu ändern:

Prozedur

1. Klicken Sie im Abschnitt "Einstellungen" auf **Show Permissions**.

   Auf der rechten Seite einer jeden Funktion wird ein Schalter angezeigt.


OfficeScan Client Settings:
Hide Permissions
Click to change the setting mode.
Centrally Managed: Settings are configured through Policy Management.
Locally Managed: Settings are configured through the product console.
More Detail
Additional Service Settings
Behavior Monitoring Settings
The settings for this section are defined locally through the product console.
Device Control Settings
Manual Scan Settings
Privileges and Other Settings

2. Klicken Sie auf den Schalter, um die Einstellungsberechtigung zu ändern.

- **Centrally Managed** (blau): Die zugewiesenen Ziele verfügen über die Einstellungen, die in der Richtlinie definiert sind.
- **Locally Managed** (orange): Control Manager verteilt nicht die Einstellungen der ausgewählten Funktion auf die Ziele. Die Administratoren für verwaltete Produkte können die Einstellungen über die Produktkonsole definieren.

Hinweis

Wenn Administratoren eine Richtlinie verteilen, in der alle Funktionseinstellungen auf "lokal verwaltet" gesetzt wurden, wird der Richtlinienstatus der Ziele nicht geändert (bleibt ausstehend).

Richtlinieneinstellungen kopieren

Administratoren können die Einstellungen von einer vorhandenen Richtlinie kopieren, eine neue Richtlinie mit den gleichen Einstellungen erstellen und die Einstellungen auf verschiedene Endpunkte oder verwaltete Produkte verteilen.

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Wählen Sie eine Richtlinie aus der Liste aus.
4. Klicken Sie auf **Copy Settings**.

   Das Fenster **Copy and Create Policy** wird angezeigt.

5. Geben Sie in das Feld **Policy Name** einen Namen für die Richtlinie ein.
6. Weisen Sie der Richtlinie **Targets** zu.
7. Klicken Sie auf **Deploy**.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Eine Richtlinie bearbeiten

Administratoren können die Informationen einer Richtlinie ändern, wie z. B. Namen, Ziele und Einstellungen einer Richtlinie, ändern. Nur der Verfasser einer Richtlinie kann die Richtlinie ändern.

Control Manager unterstützt die folgenden Änderungen:

- Eine gefilterte Richtlinie ändern
- Einer angegebenen Richtlinie mehr Ziele hinzufügen
- Von einer angegebenen Richtlinie einige Ziele entfernen

Hinweis

Control Manager erlaubt nur, dass die Verfasser von Richtlinien ihre eigenen Richtlinien ändern. Lediglich das Root-Konto kann alle Richtlinien in der Liste bearbeiten.

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Klicken Sie auf einen Richtliniennamen in der Spalte **Policy**.

Das Fenster **Edit Policy** wird angezeigt.

4. Ändern Sie die Richtlinie.
5. Klicken Sie auf **Deploy**.

   Die Änderungen werden sofort übernommen.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Eine Richtlinie löschen

Administratoren können eine Richtlinie aus der Liste entfernen. Anschließend weist Control Manager die Ziele, denen die gelöschte Richtlinie zugewiesen war, neu zu, wenn die Ziele den Filterkriterien einer anderen Richtlinie entsprechen. Ziele ohne Übereinstimmung werden zu Endpunkten ohne Richtlinien, und sie behalten die Einstellungen, die von der gelöschten Richtlinie definiert wurden, es sei denn, ein Administrator für verwaltete Produkte ändert die Einstellungen.

Hinweis

Control Manager lässt nur zu, dass der Verfasser einer Richtlinie seine eigenen Richtlinien löscht. Lediglich das Root-Konto kann alle Richtlinien in der Liste löschen.

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Wählen Sie die Richtlinie aus, die gelöscht werden soll.
4. Klicken Sie auf **Delete**.

   Ein Bestätigungsfenster wird angezeigt.
5. Klicken Sie auf **OK**.

Grundlegendes zur Liste der verwalteten Server

Im Fenster **Managed Servers** werden die Server angezeigt, die von den Administratoren über die Richtlinienverwaltung verwaltet werden können. Über das Fenster können Sie verwaltete Produkte hinzufügen oder bearbeiten, die keine MCP Agents haben.

Hinweis

Wenn die Schaltfläche **Add** deaktiviert ist, unterstützt die Richtlinienverwaltung nur verwaltete Produkte, die MCP Agents verwenden.

Bei verwalteten Produkten mit MCP Agents verwendet Control Manager die Single Sign-On- (SSO-) Funktion als Standard, um auf diese Produkte zuzugreifen. Administratoren können die Authentifizierungsinformationen aus den folgenden Gründen bearbeiten:

- Die SSO-Funktion funktioniert nicht ordnungsgemäß
- Administratoren möchten mit einem anderen Konto auf das verwaltete Produkt zugreifen

TABELLE 5-8. Liste der verwalteten Server

MENÜELEMENT	BESCHREIBUNG
Server	Zeigt den Servernamen des verwalteten Produkts an.
Anzeigename	Zeigt den Server-Anzeigenamen des verwalteten Produkts an.
Product	Zeigt den Namen des verwalteten Produkts an.
Verbindungstyp	Zeigt an, wie das verwaltete Produkt bei Control Manager registriert wird. • Automatisch: Das verwaltete Produkt wird über einen MCP Agent bei Control Manager registriert. • Manuell: Ein Administrator hat das verwaltete Produkt manuell im Fenster **Managed Servers** hinzugefügt.
Letzter Bericht	Zeigt das Datum und die Uhrzeit an, als Control Manager eine Antwort vom verwalteten Produkt erhalten hat.
Aktionen	• Bearbeiten: Klicken Sie auf dieses Symbol, um die Serverinformationen zu aktualisieren. • Löschen: Klicken Sie auf dieses Symbol, um einen manuell hinzugefügten Server zu löschen. **Hinweis** Control Manager kann keine Server entfernen, die unter Verwendung von MCP Agents registriert wurden.

PolicyServer als verwaltetes Produkt zu Control Manager hinzufügen

Endpoint Encryption ermöglicht, dass Administratoren PolicyServer mit Hilfe von Trend Micro Control Manager steuern und Endpoint Encryption Agent-Richtlinien verwalten, oder mit Trend Micro OfficeScan die Endpoint Encryption AgentSoftware auf verwaltete Endpunkte verteilen.

Wenn Sie Control Manager zur Verwaltung von PolicyServer verwenden möchten, müssen Sie PolicyServer als verwaltetes Produkt hinzufügen.

Vergewissern Sie sich bevor Sie fortfahren, dass die folgenden Aufgaben abgeschlossen wurden:

1. Installieren und Konfigurieren von Control Manager.

   Die begleitende Dokumentation finden Sie unter:

   http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

2. Installieren und Konfigurieren von PolicyServer.

   Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Wichtig

Endpoint Encryption unterstützt immer nur eine einzige konfigurierte PolicyServer Instanz in Control Manager. Es ist nicht möglich, mehrere PolicyServer Konfigurationen hinzuzufügen. Wenn Sie einen anderen PolicyServer konfigurieren möchten, müssen Sie zunächst den zuvor konfigurierten PolicyServer entfernen.

Prozedur

1. Überprüfen Sie alle Systemvoraussetzungen für kompatible Produktversionen.

   Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

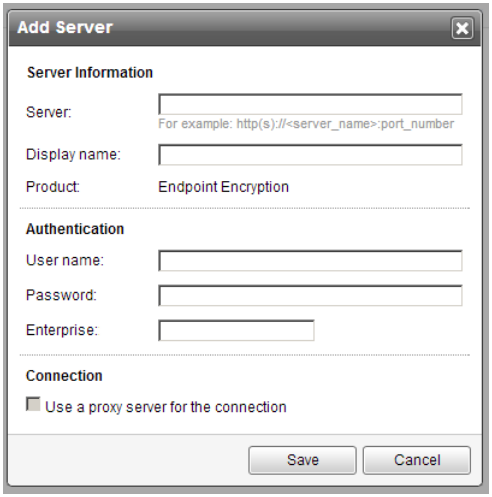
2. Melden Sie sich bei Control Manager an.

3. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Verwaltete Server**.

Das Fenster **Verwaltete Server** wird angezeigt.

4. Wählen Sie im Listenfeld **Servertyp** die Option **Endpoint Encryption**.
5. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Server hinzufügen** wird angezeigt.



6. Geben Sie die Optionen für die **Serverinformationen** an.

   - **Server**: Geben Sie den Host-Namen und die Portnummer für PolicyServer an. Verwenden Sie das folgende Format:

     ```
     http(s)://<Servername>:Portnummer
     ```

     Hinweis

     Control Manager kommuniziert mit dem PolicyServer Endpoint Encryption Dienst. Die Standardportnummer lautet 8080.

   - **Anzeigename:** Geben Sie an, wie PolicyServer im Fenster **Verwaltete Server** angezeigt wird.

7. Legen Sie unter **Authentifizierung** den Benutzernamen und das Kennwort für das Endpoint Encryption Unternehmensadministratorkonto fest.

8. Wählen Sie unter **Verbindung** den Eintrag **Einen Proxy-Server für die Verbindung verwenden**, wenn PolicyServer eine Proxy-Serververbindung erfordert.

9. Klicken Sie auf **Speichern**.

Hinweis

Die Synchronisierung zwischen Control Manager und PolicyServer dauert u. U. einige Minuten.

PolicyServer wird als neues verwaltetes Produkt zu Control Manager hinzugefügt.

Server bearbeiten

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Resources** > **Managed Servers**.

   Das Fenster **Managed Servers** wird angezeigt.

2. Klicken Sie auf das Symbol **Edit** in der Spalte **Aktionen**.

3. Bearbeiten Sie die Serverinformationen.

4. Klicken Sie auf **Save**.

Proxy-Einstellungen konfigurieren

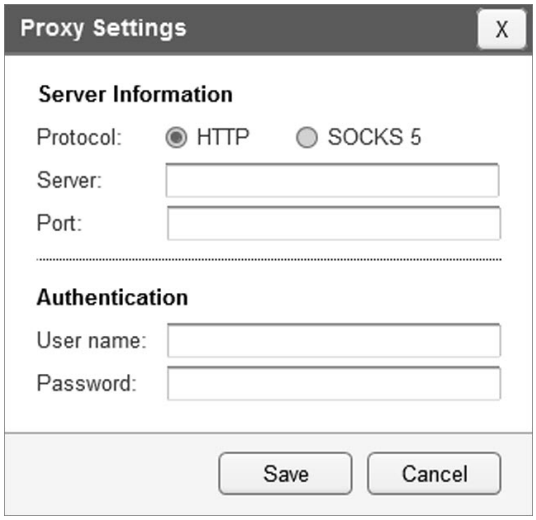
Verwenden Sie einen Proxy-Server, um eine Verbindung zu verwalteten Produkten herzustellen.

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Resources** > **Managed Servers**.

   Das Fenster **Managed Servers** wird angezeigt.

2. Klicken Sie auf **Proxy Settings**.



3. Wählen Sie das Protokoll:
   - **HTTP**
   - **SOCKS 5**
4. Geben Sie den Server-Namen in das Feld **Server** ein.
5. Geben Sie die Portnummer in das Eingabefeld **Port** ein.
6. Geben Sie den Benutzernamen und das Kennwort zum Zugriff auf den Server ein, falls eine Authentifizierung erforderlich ist.
7. Klicken Sie auf **Save**.

Richtlinienvorlagen aktualisieren

Im Fenster **Policy Template Settings** wird eine Liste der folgenden Komponenten angezeigt, mit deren Hilfe Administratoren Vorlagen aktivieren bzw. aktualisieren können:

- Framework für die Richtlinienverwaltung: Die allgemeine Richtlinienstruktur
- Produkt-Support: Die Einstellungsvorlagen für verwaltete Produkte und Endpunkte

Hinweis

Zum Überprüfen der Produktversionen, die die Richtlinienverwaltung unterstützen, bewegen Sie den Mauszeiger über das Informationssymbol in der Spalte "Template Version".

Prozedur

1. Laden Sie die neueste Komponente **Control Manager widget pool and policy templates (for Control Manager 6.0 and later)** herunter.

   In den Fenstern **Dashboard** und **Policy Management** wird oben eine blaue Benachrichtigung angezeigt.

2. Klicken Sie in einem der beiden Fenstern im Benachrichtigungsfeld auf **Update Now**.

3. Klicken Sie auf **OK**, wenn die Aktualisierung abgeschlossen ist.

   Das Fenster wird aktualisiert und das Anmeldefenster angezeigt.

4. Melden Sie sich an der Webkonsole an.

5. Navigieren Sie zu **Policies** > **Policy Resources** > **Policy Template Settings**.

   Das Fenster **Policy Template Settings** wird angezeigt.

6. Klicken Sie in der Zeile "Richtlinien-Framework" auf **Update <version number>**.

7. Zum Hinzufügen einer neuen Richtlinienvorlage klicken Sie in der Spalte "Aktion" auf **Enable**.

   Administratoren können anschließend die neuen Einstellungsvorlagen aus der Liste **Product** im Fenster **Policy Management** auswählen.

8. Zum Aktualisieren einer vorhandenen Vorlage klicken Sie in der Spalte "Aktion" auf **Update <version number>**.

Hinweis

Wenn Sie weitere Informationen zur Aktualisierung anzeigen möchten, klicken Sie in der Spalte "Aktion" auf **Details**.

Im Anschluss an die Aktualisierung können Administratoren die aktualisierten Funktionen durch Bearbeiten der vorhandenen Richtlinien überprüfen. Unter dem Abschnitt "Einstellungen" wird eine rote Meldung neben dem Titel der neuen Funktion angezeigt.

Kapitel 6

Benutzer in Control Manager

Endpoint Encryption verfügt über mehrere Typen von Kontorollen und Authentifizierungsmethoden, die eine umfassende, auf Identität basierende Authentifizierung und Verwaltung möglich machen. Mit Control Manager oder PolicyServer MMC können Sie Benutzerkonten hinzufügen oder importieren, die Authentifizierung steuern, mit Active Directory eine Synchronisierung durchführen und die Mitgliedschaft in Richtliniengruppen bei Bedarf verwalten.

In diesem Kapitel werden die Kontorollen und Authentifizierungsmethoden, die Administrierung von Control Manager zur Verwaltung von Richtlinien, die sich auf Endpoint Encryption Benutzer auswirken, und die Steuerung des Informationszugriffs über das spezialisierte Widget **Endpoint Encryption Benutzer** beschrieben. In diesem Kapitel wird ferner beschrieben, wie Sie mit Hilfe von PolicyServer MMC gelöschte Endpoint Encryption Benutzer wiederherstellen.

Hinweis

Eine Beschreibung zu Benutzerrollen und Authentifizierung von Endpoint Encryption finden Sie unter *Endpoint Encryption Benutzer auf Seite 2-5*.

Es werden folgende Themen behandelt:

- *Widget Endpoint Encryption Benutzer auf Seite 4-10*
- *Benutzer zu Endpoint Encryption hinzufügen auf Seite 6-4*

- *Benutzer suchen auf Seite 6-10*
- *Benutzer ändern auf Seite 6-10*
- *Arbeiten mit Kennwörtern auf Seite 6-11*
- *Mit Richtlinienmitgliedschaft arbeiten auf Seite 6-17*

Widget Endpoint Encryption Benutzer

Das Widget **Endpoint Encryption Benutzer** stellt Funktionen für die Benutzerverwaltung direkt vom Dashboard von Control Manager bereit. Mit dem Widget **Endpoint Encryption Benutzer** fügen Sie Endpoint Encryption Benutzerkonten hinzu oder entfernen sie, setzen Kennwörter zurück, ändern Berechtigungen, konfigurieren die Priorität der Richtliniengruppen, importieren aus Active Directory und suchen nach bestimmten Benutzerkonten.

Hinweis

Informationen zur Verwaltung von Benutzern mit dem Widget **Endpoint Encryption Benutzer** finden Sie unter *Benutzer in Control Manager auf Seite 6-1*.

Informationen, wie Sie vorhandene Endpoint Encryption Benutzer zu einer Richtlinie hinzufügen, finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

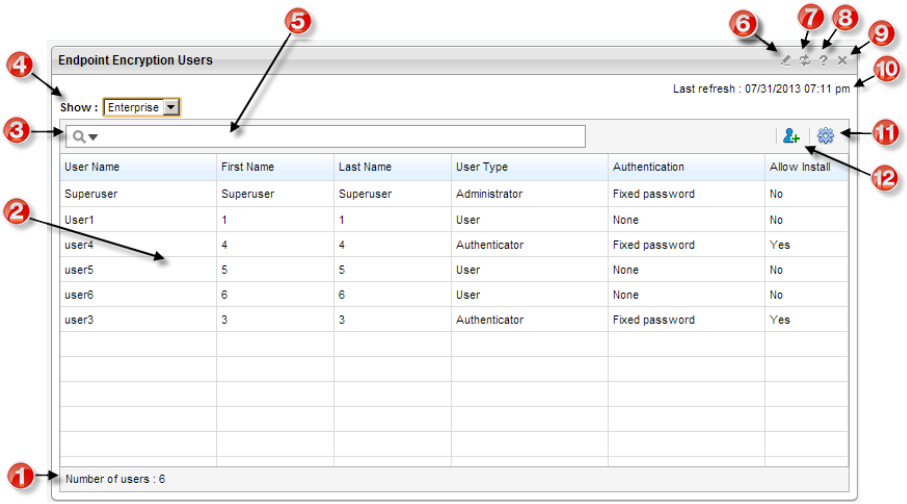


ABBILDUNG 6-1. Widget Endpoint Encryption Benutzer

TABELLE 6-1. Beschreibung des Widgets Endpoint Encryption Benutzer

VORGANG	BESCHREIBUNG
1	Zeigt die Gesamtzahl der Benutzer im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.
2	Alle Benutzer im Unternehmen, der ausgewählten Richtlinie oder der angegebenen Suche.
3	Klicken Sie auf das -Symbol, um zu filtern, welche Endpoint Encryption Benutzer in der Tabelle angezeigt werden.
4	Klicken Sie auf das Listenfeld **Anzeigen**, um das Unternehmen oder eine bestimmte Richtlinie auszuwählen, die in der Tabelle angezeigt wird.
5	Über das Suchfeld legen Sie Parameter für die Suche fest.
6	Klicken Sie auf das -Symbol, um die Widget-Einstellungen zu konfigurieren.
7	Klicken Sie auf das -Symbol, um die Widget-Daten zu aktualisieren.
8	Klicken Sie auf das -Symbol, um die Online-Hilfe anzuzeigen.
9	Klicken Sie auf das -Symbol, um das Widget zu schließen.
10	Zeigen Sie an, wann das Widget zum letzten Mal Daten mit PolicyServer synchronisiert hat.
11	Klicken Sie auf das -Symbol, um die Benutzerattribute anzuzeigen oder Aktionen für einen beliebigen ausgewählten Benutzer auszuführen.
12	Klicken Sie auf das -Symbol, um einzelne Benutzer hinzuzufügen oder um Benutzer aus einer CSV-Datei oder aus Active Directory LDAP zu importieren.

Benutzer zu Endpoint Encryption hinzufügen

Endpoint Encryption verfügt über mehrere Möglichkeiten, um Benutzer zu Endpoint Encryption hinzuzufügen:

- Fügen Sie die Benutzer manuell nacheinander hinzu.

- Verwenden Sie die Massenimportfunktion für mehrere Benutzer mit einer CSV-Datei.
- Verwenden Sie den externen Verzeichnis-Browser mit Active Directory.

Neuen Unternehmensbenutzer hinzufügen

Prozedur

1. Klicken Sie auf dem Widget **Endpoint Encryption Benutzer** auf das -Symbol, und wählen Sie anschließend **Neuen Benutzer hinzufügen**.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

2. Geben Sie die Details für das neue Benutzerkonto an:

   - **Benutzername**
   - **Vorname**
   - **Nachname**
   - **Mitarbeiter-ID**
   - **E-Mail-Adresse**
   - **Einfrieren**
   - **Benutzertyp**
   - **Eine Richtlinie**
   - **Authentifizierungsmethode**

   Hinweis

   Informationen zu den Konfigurationsoptionen finden Sie unter *Optionen zum Hinzufügen neuer Benutzer auf Seite 6-6*.

3. Klicken Sie auf **Hinzufügen**.

Der neue Benutzer wird dem Unternehmen hinzugefügt. Informationen, wie Sie den Benutzer einer Richtlinie zuweisen, finden Sie unter *Vorhandenen Benutzer zu einer Richtlinie hinzufügen auf Seite 6-22*.

Optionen zum Hinzufügen neuer Benutzer

In der folgenden Tabelle werden die verfügbaren Optionen beim Hinzufügen eines neuen Endpoint Encryption Benutzers beschrieben.

TABELLE 6-2. Optionen zum Hinzufügen neuer Benutzer

OPTIONEN	BESCHREIBUNG
Benutzername	Geben Sie den Namen des Benutzerkontos ein, den der Benutzer bei der Authentifizierung verwendet.
Vorname	Geben Sie den Vornamen des Benutzers an.
Nachname	Geben Sie den Nachnamen des Benutzers an.
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers (optional) an.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers (optional) an.
Einfrieren	Wählen Sie **Ja**, um das Konto vorübergehend zu sperren. Ein gesperrtes Konto kann sich nicht bei Endpoint Encryption Geräten anmelden.
Benutzertyp	Wählen Sie **Benutzer**, **Authentifizierer** oder **Administrator**.
Eine Gruppe	Wenn Sie **Ja** wählen, kann der Benutzer jeweils nur einer Richtlinie angehören.
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode, die für den Benutzer verfügbar ist.

Benutzer aus einer CSV-Datei importieren

Formatieren Sie jede Zeile in der CSV-Datei wie folgt:

Benutzer-ID (erforderlich), Vorname, Nachname, Mitarbeiter-ID, E-Mail-Adresse

In Feldern ohne Daten verwenden Sie ein Komma als Platzhalter.

Beispiel: Benutzer-ID,„ Mitarbeiter-ID, E-Mail-Adresse

Prozedur

1. Klicken Sie im Widget **Endpoint Encryption Benutzer** auf **Benutzer hinzufügen**, und wählen Sie anschließend **Benutzer aus einer CSV-Datei importieren**.

   Das Fenster **Benutzer aus einer CSV-Datei importieren** wird angezeigt.

2. Klicken Sie auf **Datei wählen**, um die CSV-Datei auszuwählen.

   Das Fenster **CSV-Datei öffnen** wird angezeigt.

3. Wählen Sie die Datei, und klicken Sie anschließend auf **Öffnen**.

4. Klicken Sie auf **Hinzufügen**.

Die Benutzer in der CSV-Datei werden importiert.

Active Directory-Benutzer importieren

PolicyServer beinhaltet ein Benutzerverzeichnis getrennt von der Active Directory-Datenbank. Damit kann PolicyServer absolute Sicherheit für den Zugriff auf alle Endpoint Encryption Geräte, Benutzerrechte und Authentifizierungsmethoden gewährleisten.

Informationen zur Konfiguration der Active Directory-Integration finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Prozedur

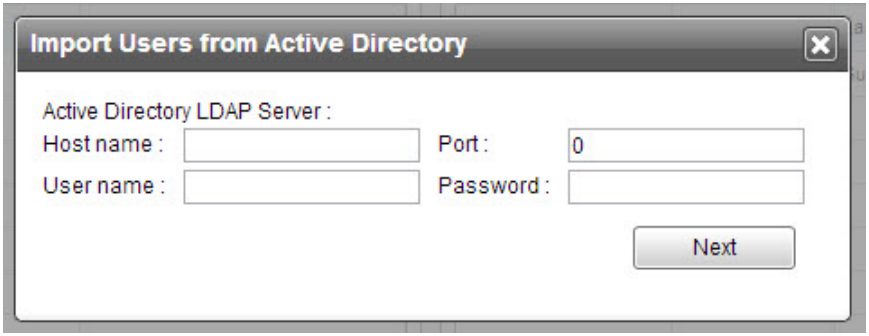
1. Melden Sie sich bei Control Manager an.

2. Navigieren Sie zum Widget **Endpoint Encryption Benutzer**.

3. Klicken Sie auf das -Symbol.

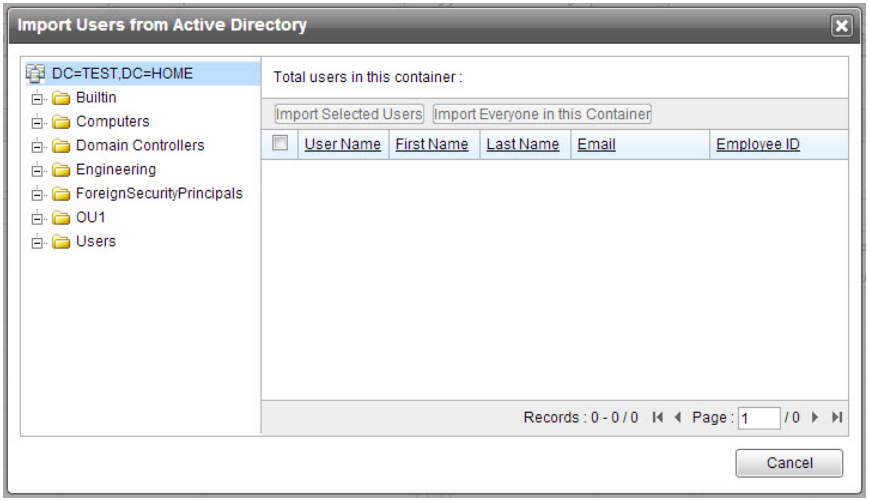
4. Wählen Sie **Benutzer aus Active Directory importieren**

Das Fenster **Benutzer aus Active Directory importieren** wird angezeigt.



5. Geben Sie die folgenden Parameter für den Active Directory-LDAP-Server an:
   - **Host-Name**
   - **Port**
   - **Benutzername**
   - **Kennwort**
6. Klicken Sie auf **Weiter**.
7. Warten Sie darauf, dass die angegebe Active Directory-Domäne mit Daten gefüllt wird.

Die Active Directory-Struktur für die angegebene Domäne wird im linken Fensterbereich angezeigt.



8. Wählen Sie in der Navigationsstruktur im linken Fensterbereich den Container, dem Benutzer hinzugefügt werden sollen.

   Die verfügbaren Benutzer werden im rechten Fensterbereich eingefügt.

9. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie einzelne Benutzer, und klicken Sie anschließend auf **Ausgewählte Benutzer importieren**.
   - Klicken Sie auf **Alle Benutzer in diesem Container importieren**.

10. Klicken Sie auf **OK**, um die Benutzer zum angegebenen Speicherort hinzuzufügen.

    Eine Bestätigungsmeldung wird angezeigt.

11. Klicken Sie zur Bestätigung auf **OK**.

    Eine Importstatusmeldung wird angezeigt.

12. Klicken Sie auf **Schließen**, um den Schritt zu beenden, oder wiederholen Sie das Verfahren, um weitere Benutzer zum Importieren auszuwählen.

Benutzer suchen

Eine Beschreibung des Widgets **Endpoint Encryption Benutzer** finden Sie unter *Widget Endpoint Encryption Benutzer auf Seite 4-10*.

Hinweis

Wenn Sie einen Benutzer zum Unternehmen hinzufügen, wird dem neuen Benutzerkonto kein Richtlinienziel zugewiesen.

Prozedur

1. Über das Listenfeld **Anzeigen** können Sie festlegen, ob Daten für das gesamte Unternehmen oder nur ausgewählte Richtlinienziele angezeigt werden.
2. Klicken Sie auf das -Symbol, um zu filtern, welche Endpoint Encryption Benutzer in der Tabelle angezeigt werden.
3. Legen Sie die Suchkriterien fest, und drücken Sie anschließend die EINGABETASTE.

Alle mit diesen Suchkriterien übereinstimmenden Benutzer werden angezeigt.

Benutzer ändern

Prozedur

1. Wählen Sie das Benutzerkonto.

   Weitere Informationen finden Sie unter *Benutzer suchen auf Seite 6-10*.

2. Wählen Sie eine der folgenden Optionen:

- Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus: **Benutzer ändern**
- Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend die folgende Option: **Benutzer ändern**

Das Fenster **Benutzer ändern** wird angezeigt.

3. Geben Sie die Änderungen an, und klicken Sie anschließend auf **Änderungen speichern**.

   Informationen zu den Konfigurationsoptionen finden Sie unter *Optionen zum Hinzufügen neuer Benutzer auf Seite 6-6*.

Arbeiten mit Kennwörtern

Wenn ein Benutzer das Kennwort vergisst oder ein Endpunkt abhanden kommt, kann der Benutzer das Kennwort unter Verwendung der durch die Richtlinien definierten Methoden zurücksetzen. Die folgenden Methoden zum Zurücksetzen von Kennwörtern stehen zur Verfügung:

- Microsoft Windows Active Directory
- Control Manager
- PolicyServer MMC
- Remote-Hilfe
- Selbsthilfe

Bei allen genannten Optionen ist es ggf. erforderlich, die Richtlinie auf Unternehmens- oder Gruppen-/Richtlinienebene festzulegen. Verwenden Sie die Richtlinie "Support-Informationen", um Benutzern Informationen zum Zurücksetzen von Kennwörtern zur Verfügung zu stellen.

Hinweis

Informationen zur Konfiguration der Support-Informationen in Control Manager finden Sie unter *Endpoint Encryption Richtlinieneinstellungen auf Seite 5-14*.

Informationen zur Konfiguration der Support-Informationen in PolicyServer MMC finden Sie unter *Setup für Support-Informationen auf Seite 11-31*.

Unternehmensadministrator-/Authentifiziererkennwort ändern

Hinweis

Es ist nicht möglich, die Kennwörter von mehreren Benutzern gleichzeitig zu ändern.

Prozedur

1. Wählen Sie im Listenfeld **Anzeigen** den Eintrag **Unternehmen**.
2. Wählen Sie das Benutzerkonto.

   Weitere Informationen finden Sie unter *Benutzer suchen auf Seite 6-10*.
3. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus:

     Kennwort ändern

   - Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das ⚙-Symbol, und wählen Sie anschließend die folgende Option:

     Kennwort ändern

   Hinweis

   In der Spalte **Benutzertyp** suchen Sie nach der entsprechenden Kontorolle.

Das Fenster **Kennwort ändern** wird angezeigt.

4. Geben Sie die Einstellungen für das neue Kennwort ein.
5. Klicken Sie auf **Speichern**.

Richtlinienadministrator-/Authentifiziererkennwort zurücksetzen

Die Änderung des Kennworts wirkt sich nur auf die Kombination aus Benutzername und Kennwort für die aktuelle Richtliniengruppe aus. Kennwörter der Richtliniengruppe sind eindeutig und müssen sich von Kennwörtern für andere Richtliniengruppen unterscheiden. Um das Kennwort für das Benutzerkonto über alle Richtliniengruppen hinweg zu ändern, müssen Sie das Kontokennwort auf Unternehmensebene ändern.

Prozedur

1. Wählen Sie im Listenfeld **Anzeigen** den Eintrag den entsprechenden Richtliniennamen.
2. Wählen Sie das Benutzerkonto.

   Informationen über die Suche nach dem Konto finden Sie unter *Benutzer suchen auf Seite 6-10*.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus:

     Kennwort ändern
   - Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend die folgende Option:

     Kennwort ändern

Hinweis

In der Spalte **Benutzertyp** suchen Sie nach der entsprechenden Kontorolle.

Das Fenster **Kennwort ändern** wird angezeigt.

4. Geben Sie die Einstellungen für das neue Kennwort ein.

5. Klicken Sie auf **Speichern**.

Ein festes Kennwort zurücksetzen

Die Änderung des Kennworts wirkt sich nur auf die Kombination aus Benutzername und Kennwort für die aktuelle Richtliniengruppe aus. Kennwörter der Richtliniengruppe sind eindeutig und müssen sich von Kennwörtern für andere Richtliniengruppen unterscheiden. Um das Kennwort für das Benutzerkonto über alle Richtliniengruppen hinweg zu ändern, müssen Sie das Kontokennwort auf Unternehmensebene ändern.

Prozedur

1. Wählen Sie im Listenfeld **Anzeigen** den Eintrag den entsprechenden Gruppennamen.

2. Wählen Sie das Benutzerkonto.

   Informationen über die Suche nach dem Konto finden Sie unter *Benutzer suchen auf Seite 6-10*.

3. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus:

     Kennwort ändern

   - Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das ⚙-Symbol, und wählen Sie anschließend die folgende Option:

     Kennwort ändern

Hinweis

In der Spalte **Benutzertyp** suchen Sie nach der entsprechenden Kontorolle.

Das Fenster **Kennwort ändern** wird angezeigt.

4. Vergewissern Sie sich, dass im Listenfeld **Authentifizierungsmethode** der Eintrag **Festes Kennwort** ausgewählt ist.
5. Geben Sie das neue feste Kennwort ein.
6. Bestätigen Sie das neue feste Kennwort.
7. Klicken Sie auf **Speichern**.

Domänenauthentifizierung für einen Benutzer aktivieren

Falls konfiguriert, können sich Benutzer mit den Anmeldedaten von Active Directory authentifizieren. Es ist nicht möglich, das Active Directory-Kennwort zu ändern.

Prozedur

1. Wählen Sie im Listenfeld **Anzeigen** den Eintrag den entsprechenden Gruppennamen.
2. Wählen Sie das Benutzerkonto.

   Informationen über die Suche nach dem Konto finden Sie unter *Benutzer suchen auf Seite 6-10*.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus:

     Kennwort ändern
   - Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das ⚙-Symbol, und wählen Sie anschließend die folgende Option:

     Kennwort ändern

Hinweis

In der Spalte **Benutzertyp** suchen Sie nach der entsprechenden Kontorolle.

Das Fenster **Kennwort ändern** wird angezeigt.

4. Wählen Sie im Listenfeld **Authentifizierungsmethode** die Option **Domäne**.
5. Klicken Sie auf **Speichern**.

Für einen Benutzer feste Kennwörter aktivieren

Die Änderung des Kennworts wirkt sich nur auf die Kombination aus Benutzername und Kennwort für die aktuelle Richtliniengruppe aus. Kennwörter der Richtliniengruppe sind eindeutig und müssen sich von Kennwörtern für andere Richtliniengruppen unterscheiden. Um das Kennwort für das Benutzerkonto über alle Richtliniengruppen hinweg zu ändern, müssen Sie das Kontokennwort auf Unternehmensebene ändern.

Prozedur

1. Wählen Sie im Listenfeld **Anzeigen** den entsprechenden Gruppennamen.
2. Wählen Sie das Benutzerkonto.

   Informationen über die Suche nach dem Konto finden Sie unter *Benutzer suchen auf Seite 6-10*.
3. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus:

     Kennwort ändern

   - Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das ⚙-Symbol, und wählen Sie anschließend die folgende Option:

     Kennwort ändern

Hinweis

In der Spalte **Benutzertyp** suchen Sie nach der entsprechenden Kontorolle.

Das Fenster **Kennwort ändern** wird angezeigt.

4. Wählen Sie im Listenfeld **Authentifizierungsmethode** den Eintrag **Festes Kennwort**.
5. Geben Sie das feste Kennwort ein.
6. Bestätigen Sie das feste Kennwort.
7. Klicken Sie auf **Speichern**.

Mit Richtlinienmitgliedschaft arbeiten

In diesem Abschnitt wird erklärt, wie Sie Benutzer einer Richtliniengruppe hinzufügen oder daraus entfernen und wie Sie einen gelöschten Benutzer wiederherstellen.

Gruppen

Um die Richtlinienverwaltung zu rationalisieren, führt Control Manager die PolicyServer MMC Gruppen- und Richtlinienhierarchie zusammen. Unabhängig von der von Ihnen bevorzugten Management-Konsole behält PolicyServer dieselbe Richtlinien- und Gruppenkonfiguration bei. Wenn Sie in Control Manager ein neues Richtlinienziel erstellen, zeigt PolicyServer MMC eine neue Gruppe an, die die Richtlinienkonfigurationen und die Benutzer enthält, die der Richtlinie hinzugefügt wurden.

Wichtig

Control Manager hat immer Vorrang. Alle mit PolicyServer MMC durchgeführten Änderungen an der Gruppenzuweisung werden beim nächsten Mal automatisch überschrieben, wenn Control Manager Richtlinien mit PolicyServer synchronisiert.

Richtlinienmitgliedschaft

Die folgende Tabelle dient zum Verständnis der Mitgliedschaft in einer Endpoint Encryption Benutzerrichtlinie.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

TABELLE 6-3. Beschreibung der Richtlinienmitgliedschaften

HEADER	BEISPIEL	BESCHREIBUNG
Priorität	1, 2. 3	Zeigt die Reihenfolge an, in der Richtlinien auf den Endpoint Encryption Benutzer angewendet werden. Weitere Informationen finden Sie unter *Richtlinienpriorität für den Benutzer ändern auf Seite 6-21*.
Name der Richtlinie	GP1	Zeigt den Namen aller Richtlinien an, denen der Benutzer gegenwärtig zugewiesen ist.
Beschreibung	Richtlinie zu temporären Mitarbeitern.	Zeigt die Beschreibung der Richtlinie an. Informationen zum Ändern der Richtlinienbeschreibung finden Sie unter *Eine Richtlinie bearbeiten auf Seite 5-29*.

HEADER	BEISPIEL	BESCHREIBUNG
Installation zulassen	Ja, Nein	Zeigt an, ob der Benutzer neue Endpoint Encryption Geräte installieren kann. Weitere Informationen finden Sie unter *Einem Benutzer das Installieren von Geräten erlauben auf Seite 6-20*.

Zugewiesene Richtlinien des Benutzers anzeigen

Im Fenster **Richtlinienmitgliedschaft** zeigen Sie die Richtlinienzuweisung des Endpoint Encryption Benutzers an. Wenn Sie einem Benutzer erlauben, in eine Gruppe zu installieren, dann ist dieser Benutzer in der Lage, neue Endpoint Encryption Geräte in eine Richtliniengruppe zu installieren, indem die Endpoint Encryption Agent-Software auf dem Endpunkt installiert wird. Die Änderung der Priorität wirkt sich auf die Richtlinienmitgliedschaft der neuen Endpoint Encryption Geräte aus, wenn der Benutzer den Endpoint Encryption Agent installiert. Bei der Richtlinie mit der höchsten Priorität (1) handelt es sich um die Standardrichtlinie.

Prozedur

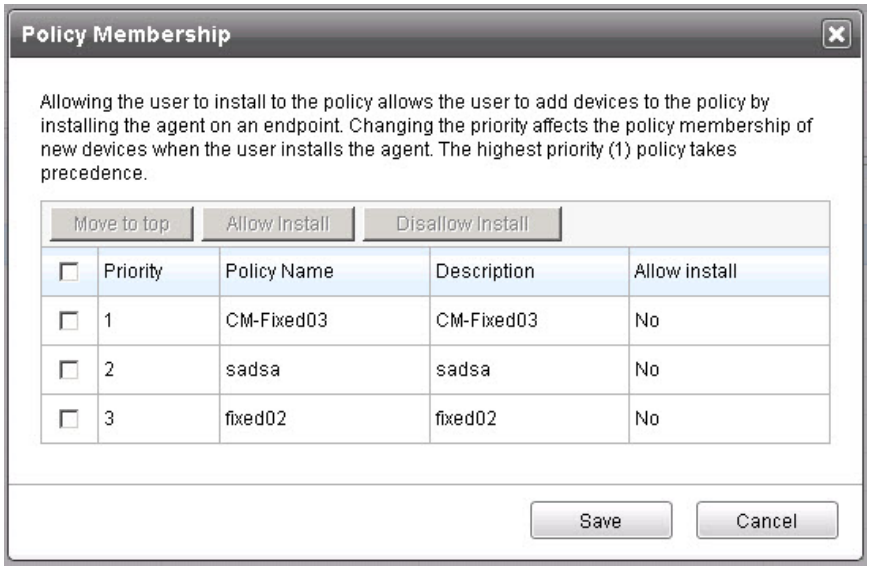
1. Wählen Sie das Benutzerkonto.

   Informationen über die Suche nach dem Konto finden Sie unter *Benutzer suchen auf Seite 6-10*.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf den Benutzer in der Tabelle, und wählen Sie die folgende Option aus: **Richtlinien auflisten**
   - Wählen Sie den Benutzer in der Tabelle, klicken Sie auf das ⚙-Symbol, und wählen Sie anschließend die folgende Option: **Richtlinien auflisten**

Das Fenster **Richtlinienmitgliedschaft** wird angezeigt.



3. Sie können optional die Richtlinienzuweisung ändern.

   a. Aktivieren Sie das Kontrollkästchen neben der entsprechenden Richtlinie.

   b. Klicken Sie auf **Installation zulassen**.

   c. Klicken Sie auf **Speichern**.

Einem Benutzer das Installieren von Geräten erlauben

Mit dieser Option wird es Endpoint Encryption Benutzern ermöglicht, Endpoint Encryption Geräte einer Richtlinie hinzufügen, ohne die Richtlinienadministrator-/Authentifiziererberechtigungen für die Richtlinie zu besitzen. Der Standardwert ist **Nein**.

Prozedur

1. Navigieren Sie zur Richtlinienliste für den Endpoint Encryption Benutzer.

   Weitere Informationen finden Sie unter *Zugewiesene Richtlinien des Benutzers anzeigen auf Seite 6-19*.

2. Aktivieren Sie das Kontrollkästchen neben der entsprechenden Richtlinie, damit der Benutzer in der Lage ist, Geräte zu installieren.

3. Klicken Sie auf **Client-Installation zulassen**.

Richtlinienpriorität für den Benutzer ändern

Die Richtlinienpriorität definiert die Reihenfolge, in der Richtlinien angewendet werden, wenn sich ein Benutzer am Gerät anmeldet. Die erste Richtlinie in der Richtlinienliste ist die Standardrichtlinie für den Benutzer. Wenn ein Benutzer ein Gerät installiert, wird das Gerät immer der Standardrichtlinie des Benutzers zugeordnet.

Hinweis

Der Benutzer muss dazu berechtigt sein, in die Standardgruppe zu installieren. Weitere Informationen finden Sie unter *Einem Benutzer das Installieren von Geräten erlauben auf Seite 6-20*.

Prozedur

1. Navigieren Sie zur Richtlinienliste für den Benutzer.

   Weitere Informationen finden Sie unter *Zugewiesene Richtlinien des Benutzers anzeigen auf Seite 6-19*.

2. Aktivieren Sie das Kontrollkästchen neben der Richtlinie, um diese als Standardrichtlinie festzulegen.

3. Klicken Sie auf **An den Anfang verschieben**.

Neuen Benutzer zu einer Richtlinie hinzufügen

Sie können nur vorhandene Benutzer zu einer Richtlinien hinzufügen. Um einen Benutzer hinzuzufügen, fügen Sie zuerst einen neuen Benutzer mit dem Widget **Endpoint Encryption Benutzer** hinzu, und fügen Sie anschließend das Benutzerkonto der Richtlinie hinzu. Es ist nicht möglich, einen neuen Benutzer einer Richtlinie mit dem Widget **Endpoint Encryption Benutzer** direkt zuzuweisen.

Prozedur

1. Erstellen Sie den neuen Benutzer mit dem Widget **Endpoint Encryption Benutzer**.

   Weitere Informationen finden Sie unter *Neuen Unternehmensbenutzer hinzufügen auf Seite 6-5*.

2. Fügen Sie den Benutzer einer Richtlinie hinzu.

   Weitere Informationen finden Sie unter *Vorhandenen Benutzer zu einer Richtlinie hinzufügen auf Seite 6-22*.

Vorhandenen Benutzer zu einer Richtlinie hinzufügen

Es ist nicht möglich, einen neuen Benutzer einer Richtlinie mit dem Widget **Endpoint Encryption Benutzer** direkt zuzuweisen.

Hinweis

Informationen über die verfügbaren Benutzeroptionen in der Richtlinie finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

Administratoren können die Informationen einer Richtlinie ändern, wie z. B. Namen, Ziele und Einstellungen einer Richtlinie, ändern. Nur der Verfasser einer Richtlinie kann die Richtlinie ändern.

Control Manager unterstützt die folgenden Änderungen:

- Eine gefilterte Richtlinie ändern

- Einer angegebenen Richtlinie mehr Ziele hinzufügen
- Von einer angegebenen Richtlinie einige Ziele entfernen

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

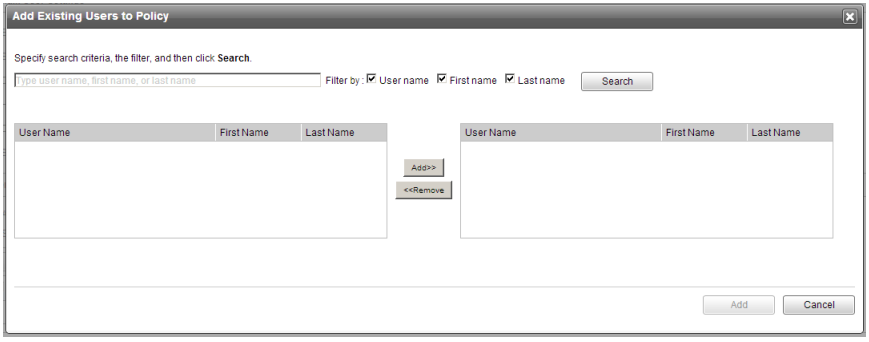
3. Klicken Sie auf einen Richtliniennamen in der Spalte **Policy**.

   Das Fenster **Edit Policy** wird angezeigt.

4. Wählen Sie im Abschnitt **Benutzer** die Option **Bestimmte Benutzer auswählen**.

5. Klicken Sie auf **Benutzer auswählen**.

   Das Fenster **Vorhandene Benutzer zur Richtlinie hinzufügen** wird angezeigt.



6. Geben Sie die Suchkriterien ein, und klicken Sie dann auf **Suchen**.

   Alle Benutzer, die den Suchkriterien entsprechen, werden im linken Fensterbereich angezeigt.

7. Wenn Sie einen Benutzer der Richtlinie hinzufügen möchten, wählen Sie den Benutzer im linken Fensterbereich aus, und klicken Sie anschließend auf **Hinzufügen>>**.

   Das Benutzerkonto wird in den rechten Fensterbereich verschoben.

8. Wenn Sie einen Benutzer aus der Auswahl entfernen möchten, wählen Sie den Benutzer im rechten Fensterbereich aus, und klicken Sie anschließend auf **<<Entfernen**.

   Das Benutzerkonto wird in den linken Fensterbereich verschoben.

9. Klicken Sie auf **Hinzufügen**.

10. Klicken Sie auf **Deploy**.

    Die Änderungen werden sofort übernommen.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Benutzer aus einer Richtlinie entfernen

Warnung!

- Bevor Sie den Administrator oder Authentifizierer entfernen, weisen Sie diese Rolle einem anderen Endpoint Encryption Benutzer zu. Andernfalls können nur der Unternehmensadministrator oder der Unternehmensauthentifizierer Änderungen an der Richtlinie vornehmen.
- Wenn Sie Endpoint Encryption Benutzer aus einer Richtline entfernen, sind diese Benutzer nicht mehr in der Lage, auf die verschlüsselten Endpoint Encryption Geräte zuzugreifen, die dieser Richtlinie zugeordnet sind. Bevor Sie Benutzer entfernen, vergewissern Sie sich, dass diese ihre Daten gesichert und entschlüsselt haben.

Es ist nicht möglich, einen Benutzer mit dem Widget "Endpoint Encryption Benutzer" aus einer Richtlinie zu entfernen. Informationen zu den verfügbaren Benutzeroptionen finden Sie unter *Regeln für Endpoint Encryption Benutzer konfigurieren auf Seite 3-16*.

Administratoren können die Informationen einer Richtlinie ändern, wie z. B. Namen, Ziele und Einstellungen einer Richtlinie, ändern. Nur der Verfasser einer Richtlinie kann die Richtlinie ändern.

Control Manager unterstützt die folgenden Änderungen:

- Eine gefilterte Richtlinie ändern
- Einer angegebenen Richtlinie mehr Ziele hinzufügen
- Von einer angegebenen Richtlinie einige Ziele entfernen

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Klicken Sie auf einen Richtliniennamen in der Spalte **Policy**.

   Das Fenster **Edit Policy** wird angezeigt.

4. Ändern Sie die Richtlinie.

5. Wählen Sie alle Benutzer, die aus der Richtlinie entfernt werden sollen, und klicken Sie anschließend auf **Benutzer aus Richtlinie entfernen**.

6. Klicken Sie auf **Deploy**.

   Die Änderungen werden sofort übernommen.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Alle Benutzer aus einer Richtlinie entfernen

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Klicken Sie auf einen Richtliniennamen in der Spalte **Policy**.

   Das Fenster **Edit Policy** wird angezeigt.

4. Erweitern Sie den Abschnitt **Benutzer**, und wählen Sie anschließend **Bestimmte Benutzer auswählen**, falls noch nicht ausgewählt.

5. Wählen Sie alle Benutzerkonten, und wählen Sie anschließend **Benutzer entfernen**.

   Alle Benutzer wurde aus der Richtlinie entfernt.

6. Klicken Sie auf **Deploy**.

   Die Änderungen werden sofort übernommen.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Gelöschtes Benutzer wiederherstellen

In Umgebungen mit Control Manager und PolicyServer MMC können Sie gelöschte Endpoint Encryption Benutzer mit dem Papierkorb-Knoten von PolicyServer MMC wiederherstellen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie den **Papierkorb**.
3. Öffnen Sie **Gelöschte Benutzer**.

   Im rechten Fenster werden alle gelöschten Benutzer geladen.
4. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto, und wählen Sie anschließend **Benutzer wiederherstellen**.

   Der Benutzer wird wieder zum Unternehmen hinzugefügt, gehört jedoch keiner Richtliniengruppe an.

Kapitel 7

Geräte in Control Manager

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die bei PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

In diesem Kapitel wird erklärt, wie Sie Control Manager administrieren, um Richtlinien zu verwalten, die sich auf Endpoint Encryption Geräte auswirken, und wie Sie die Datensicherheit mit Hilfe des spezialisierten Widgets für Endpoint Encryption Geräte gewährleisten. In diesem Kapitel wird ferner beschrieben, wie Sie mit Hilfe von PolicyServer MMC gelöschte Endpoint Encryption Geräte wiederherstellen.

Es werden folgende Themen behandelt:

- *Gerät zu einer Richtlinie hinzufügen auf Seite 7-3*
- *Gerät aus einer Richtlinie entfernen auf Seite 7-6*
- *Widget Endpoint Encryption - Geräte auf Seite 4-12*
- *Ein Gerät suchen auf Seite 7-9*
- *Gerät aus dem Unternehmen löschen auf Seite 7-17*
- *Ein Software-Token abrufen auf Seite 7-10*

- *Wiederherstellungsschlüssel abrufen auf Seite 7-11*
- *Geräteattribute anzeigen auf Seite 7-12*
- *Gerät auslöschen auf Seite 7-15*
- *Gerät sperren auf Seite 7-16*
- *Ein Gerät zurücksetzen auf Seite 7-17*
- *Gelöschtes Gerät wiederherstellen auf Seite 7-19*

Gerät zu einer Richtlinie hinzufügen

Endpoint Encryption Geräte werden automatisch der Standardrichtlinie hinzugefügt, die dem Benutzer zugeordnet ist, der den Endpoint Encryption Agent auf dem Endpunkt installiert hat. Wenn Sie Endpoint Encryption Geräte manuell zu Richtlinien in Control Manager hinzufügen möchten, weisen Sie dieser Richtlinie Ziele zu. Das folgende Verfahren beschreibt, wie Sie Endpoint Encryption Geräte einer vorhandenen Control Manager Richtlinie hinzufügen. Informationen zum Hinzufügen einer neuen Richtlinie finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

Hinweis

Jedes Endpoint Encryption Gerät kann nur einer einzigen Richtlinie angehören.

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Klicken Sie auf einen Richtliniennamen in der Spalte **Policy**.

   Das Fenster **Edit Policy** wird angezeigt.

4. Ändern Sie die Richtlinie.

5. Aktivieren Sie eine der folgenden Optionen für das Richtlinienziel:

   - **Keines (nur Entwurf)**: Sie erstellen eine Richtlinie ohne Ziele (Endpunkte).
   - **Filter nach Kriterien**: Endpoint Encryption unterstützt keine Filterung nach Kriterien.
   - **Ziel(e) angeben**: Sie geben vorhandene Endpunkte an.

Hinweis

Weitere Informationen über Richtlinienziele finden Sie unter *Richtlinienziele angeben auf Seite 3-14*.

6. Klicken Sie auf **Deploy**.

   Die Änderungen werden sofort übernommen.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Richtlinienziele angeben

Im Fenster **Ziel(e) angeben** weisen Sie die Endpoint Encryption Geräte der Richtlinie zu.

Hinweis

Das Fenster **Ziel(e) angeben** wird angezeigt, wenn Sie eine neue Richtlinie erstellen. Informationen zum Erstellen einer Richtlinie finden Sie unter *Eine Richtlinie erstellen auf Seite 3-12*.

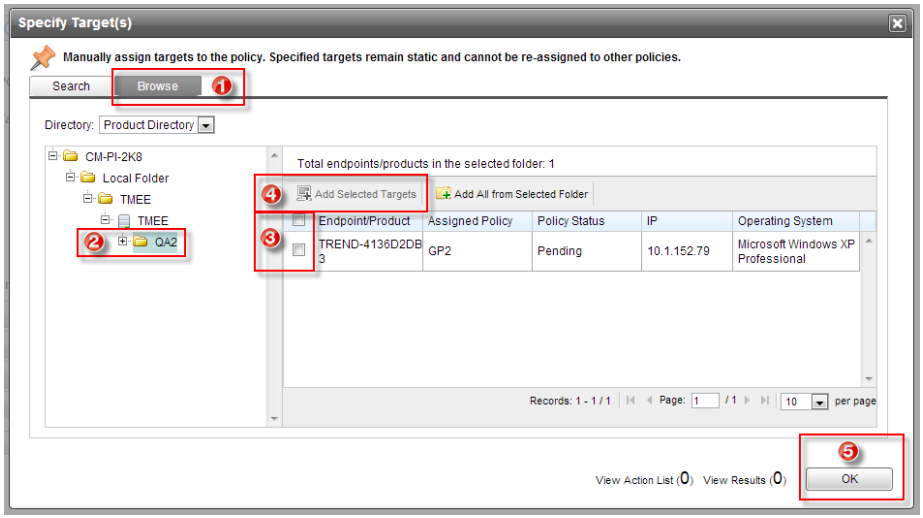


ABBILDUNG 7-1. Richtlinienziele angeben

Prozedur

1. Klicken Sie im Fenster **Ziel(e) angeben** auf die Registerkarte **Durchsuchen**.

2. Erweitern Sie die Struktur im linken Fensterbereich, um den verwalteten Ordner zu wählen.

   Beispiel: **CM-PI-2K8 > Lokaler Ordner > TMEE > TMEE > QA2**

3. Wählen Sie die entsprechenden Endpoint Encryption Geräte, oder aktivieren Sie das obere Kontrollkästchen, um alle Endpoint Encryption Geräte auszuwählen, die auf der aktuellen Seite aufgelistet werden.

4. Klicken Sie auf **Ausgewählte Ziele hinzufügen**.

Hinweis

Wenn Sie sofort alle Geräte im verwalteten Ordner auswählen möchten, klicken Sie auf **Alle aus ausgewähltem Ordner hinzufügen**.

„Aktionsliste anzeigen“ und „Ergebnisse anzeigen“ werden basierend auf der Auswahl aktualisiert.

5. Klicken Sie auf **OK**.

Gerät aus einer Richtlinie entfernen

Prozedur

1. Navigieren Sie zu **Policies** > **Policy Management**.

   Das Fenster **Policy Management** wird angezeigt.

2. Wählen Sie die Art der Produkteinstellungen aus der Liste **Product**.

   Das Fenster wird aktualisiert und zeigt die Richtlinien an, die für das ausgewählte verwaltete Produkt erstellt wurden.

3. Klicken Sie auf einen Richtliniennamen in der Spalte **Policy**.

   Das Fenster **Edit Policy** wird angezeigt.

4. Wählen Sie **Ziele angeben**.

   Weitere Informationen finden Sie unter *Richtlinienziele angeben auf Seite 3-14*.

   Hinweis

   Die Filterung nach Kriterien wird von Endpoint Encryption nicht unterstützt.

5. Klicken Sie auf **Deploy**.

   Die Änderungen werden sofort übernommen.

Hinweis

- Nachdem Sie auf **Deploy** geklickt haben, warten Sie zwei Minuten lang, bis Control Manager die Richtlinie auf die Ziele verteilt hat. Klicken Sie auf **Refresh** im Fenster **Policy Management**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Control Manager setzt die Richtlinieneinstellungen in den Zielen alle 24 Stunden durch.

Widget Endpoint Encryption - Geräte

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die bei PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

Das Widget **Endpoint Encryption - Geräte** stellt direkt im Dashboard von Control Manager Funktionen für die Endpoint Encryption Geräteverwaltung bereit. Mit dem Widget **Endpoint Encryption - Geräte** überwachen Sie Aktivitäten, suchen nach Endpoint Encryption Geräten oder sichern die Daten auf dem Endpunkt, indem Sie einen Befehl zum Sperren oder Löschen einleiten, wenn ein Endpunkt gestohlen wird oder verloren geht.

Hinweis

Informationen zur Verwaltung von Geräten mit dem Widget **Endpoint Encryption - Geräte** finden Sie unter *Geräte in Control Manager auf Seite 7-1*.

Informationen, wie Sie Endpoint Encryption Geräte zu einer Richtlinie hinzufügen, finden Sie unter *Richtlinienziele angeben auf Seite 3-14*.

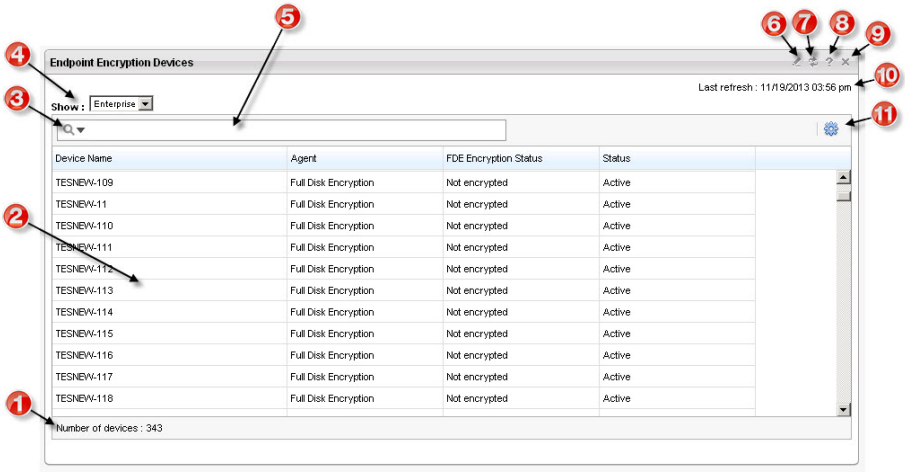


ABBILDUNG 7-2. Widget Endpoint Encryption - Geräte

TABELLE 7-1. Beschreibung des Widgets Endpoint Encryption - Geräte

VORGANG	BESCHREIBUNG
1	Zeigt die Gesamtzahl der Geräte im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.
2	Zeigt alle Geräte im gesamten Unternehmen, der ausgewählten Gruppe oder der angegebenen Suche an. • **Gerätename**: Der Computername, der dem Endpoint Encryption Gerät zugeordnet ist. • **Agent**: Der installierte Endpoint Encryption Agent. • **FDE Verschlüsselungsstatus**: Wenn Full Disk Encryption Agent installiert ist, der Verschlüsselungsstatus. Weitere Informationen finden Sie unter *Widget "Full Disk Encryption Status" auf Seite 4-15*. • **Status**: Der aktuelle Status des Endpoint Encryption Geräts.
3	Klicken Sie auf das Symbol , um den Endpoint Encryption Agent auszuwählen und die in der Tabelle angezeigten Geräte zu filtern.

VORGANG	BESCHREIBUNG
4	Klicken Sie auf das Listenfeld **Anzeigen**, um das gesamte Unternehmen oder eine bestimmte Richtlinie auszuwählen, die in der Tabelle angezeigt wird.
5	Über das Suchfeld legen Sie Parameter für die Suche fest. Sie können nach allen Attributen suchen, die in den Geräteattributen aufgeführt werden.
6	Klicken Sie auf das -Symbol, um die Widget-Einstellungen zu konfigurieren.
7	Klicken Sie auf das -Symbol, um die Widget-Daten zu aktualisieren.
8	Klicken Sie auf das -Symbol, um die Online-Hilfe anzuzeigen.
9	Klicken Sie auf das -Symbol, um das Widget zu schließen.
10	Zeigen Sie an, wann das Widget zum letzten Mal Daten mit PolicyServer synchronisiert hat.
11	Klicken Sie auf das -Symbol, um die Geräteattribute anzuzeigen oder Aktionen für ein beliebiges ausgewähltes Gerät auszuführen.

Ein Gerät suchen

Informationen über die Benutzeroberfläche des Widgets **Endpoint Encryption - Geräte** finden Sie unter *Widget Endpoint Encryption - Geräte auf Seite 4-12*.

Prozedur

1. Navigieren Sie zum Widget **Endpoint Encryption - Geräte**.
2. Führen Sie einen oder mehrere der folgenden Schritte aus:
   - Klicken Sie auf das Symbol , um den Endpoint Encryption Agent auszuwählen und die in der Tabelle angezeigten Geräte zu filtern.
   - Klicken Sie auf das Listenfeld **Anzeigen**, um das gesamte Unternehmen oder eine bestimmte Richtlinie auszuwählen, die in der Tabelle angezeigt wird.

- Über das Suchfeld legen Sie Parameter für die Suche fest. Sie können nach allen Attributen suchen, die in den Geräteattributen aufgeführt werden.

3. Suchen Sie das Gerät in der Tabelle.

Ein Software-Token abrufen

Wenn Sie ein „Software-Token“ erstellen, wird eine eindeutige Zeichenfolge erstellt, mit deren Hilfe Endpoint Encryption Geräte entsperrt werden können. Auf diese Weise können Sie die Remote-Hilfe für Endpoint Encryption Benutzer ausführen, um vergessene Kennwörter zurückzusetzen.

Hinweis

Das Software-Token ist nur in der Vollversion von Full Disk Encryption verfügbar, nicht in der Encryption Management for Apple FileVault oder Encryption Management for Microsoft BitLocker.

Informationen über die Unterstützung durch Remote-Hilfe finden Sie unter *Unterstützung durch Remote-Hilfe auf Seite 11-29*.

Prozedur

1. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

2. Klicken Sie mit der rechten Maustaste auf das Gerät, und wählen Sie **Software-Token**.

   Das Fenster **Software-Token** wird angezeigt.

3. Fragen Sie den Benutzer nach dem aus 16 Ziffern bestehenden Herausforderungscode, und geben Sie ihn in das Feld **Herausforderung** im Fenster **Software-Token** ein.

4. Klicken Sie auf **Antwort erhalten**.

Das Feld **Antwort** wird mit einer aus 8 Zeichen bestehenden Zeichenfolge geladen.

5. Teilen Sie dem Benutzer die aus 8 Zeichen bestehende Zeichenfolge über das Feld **Antwort** mit.

Das Endpoint Encryption Gerät wird entsprerrt und der Endpoint Encryption Benutzer kann sich am Gerät anmelden.

Wiederherstellungsschlüssel abrufen

Wenn Sie einen „Wiederherstellungsschlüssel“ generieren, können Benutzer eine Festplatte entschlüsseln, wenn der Benutzer das ursprüngliche Kennwort oder den ursprünglichen Schlüssel vergessen hat. Der Wiederherstellungsschlüssel ist nur für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker Agents verfügbar, weil diese keine der anderen verfügbaren Wiederherstellungsmethoden in Full Disk Encryption verwenden.

Hinweis

Der Wiederherstellungsschlüssel wird für verschlüsselte Geräte eingesetzt und ist nur als Option verfügbar, wenn die entsprechenden Geräte ausgewählt werden.

Prozedur

1. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf das Gerät in der Tabelle, und wählen Sie **Wiederherstellungsschlüssel**.
   - Wählen Sie das Gerät in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend **Wiederherstellungsschlüssel**.

   Der Wiederherstellungsschlüssel wird angezeigt.

3. Kopieren Sie den gewünschten Wiederherstellungsschlüssel auf das gesperrte Gerät.

4. Klicken Sie auf **OK**.

Geräteattribute anzeigen

Über **Geräteattribute** zeigen Sie den aktuellen Snapshot des ausgewählten Geräts an.

Prozedur

1. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf das Gerät in der Tabelle, und wählen Sie **Attribute**.
   - Wählen Sie das Gerät in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend **Attribute**.

Das Fenster **Geräteattribute** wird angezeigt.

Endpoint Encryption Geräteattribute

In der folgenden Tabelle werden die Endpoint Encryption Geräteattribute beschrieben.

TABELLE 7-2. Endpoint Encryption Geräteattribute

ATTRIBUTNAME	BEISPIEL	BESCHREIBUNG
.NET-Version	2.0.50727.3620	Die Versions- und Build-Nummer für das installierte .NET Framework

ATTRIBUTNAME	BEISPIEL	BESCHREIBUNG
Build-Nummer des Common Framework	5.0.0.84	Der Endpoint Encryption Agent verwendet ein Common Framework zur Verschlüsselung. Anhand der Build-Nummer erkennen Sie, ob der Agent aktuell ist
Modell der Festplatte	VMware Virtual IDE	Der Festplattenmodus.
Festplattenname	`\\.\PHYSICALDRIVE0`	Der Name der Festplatte.
Festplattenpartitionen	1	Die Anzahl der Partitionen auf der Festplatte, auf der der Agent installiert ist.
Größe der Festplatte	10733990400	Die Gesamtkapazität der Festplatte (Byte).
Domänenname	WORKGROUP	Die Domäne, zu der der Endpunkt gehört.
Endpunkt-ID	85b1e3e2a3c25d882540ef6e4818c3e4	Die eindeutige ID des Endpunkts, die zur Control Manager Integration verwendet wird.
<Agent> Benutzer	maryjane	Der Benutzername des zuletzt angemeldeten Benutzers.
<Agent> Version	5.0.0.260	Die Versions- und die Build-Nummer für die Agent-Installation.
Host-Name	TREND-4136D2DB3	Der Host-Name des Endpunkts.
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpunkts.

Attributname	Beispiel	Beschreibung
Gebietsschema	Deutsch (Deutschland)	Die Sprache und die Region, für die der Endpunkt konfiguriert wurde.
Computername	TREND-4136D2DB3	Der Computername, den dieser Endpunkt verwendet.
Hersteller	VMware, Inc.	Der Hersteller der Festplatte.
Modell	Virtuelle VMware-Plattform	Das Modell der Festplatte.
Betriebssystem	Microsoft Windows NT 5.1.2600 Service Pack 3	Das Betriebssystem, das auf derselben Festplatte wie der Agent installiert ist.
Name des Betriebssystems	Microsoft Windows XP Professional	Der allgemeine Name des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Service Pack des Betriebssystems	Service Pack 3	Die Nummer des Service-Packs des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Version des Betriebssystems	5.1.2600.196608	Die Versionsnummer des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Partitionsschema	Klassischer MBR	Das Partitionsschema für die Festplatte.
Prozessor	x86 Family 6 Modell 30 Stepping 5, Genuine Intel	Marke und Modell des Prozessors auf dem Endpunkt.
Prozessoranzahl	2	Die Anzahl der Prozessoren im Endpunkt.

Attributname	Beispiel	Beschreibung
Prozessorrevision	1e05	Die Prozessorrevisionsnummer.
Zeitzone	Taipei Standardzeit	Die Zeitzone, in der sich der Endpunkt befindet.
Gesamter physischer Arbeitsspeicher	2.047MB	Die Gesamtmenge des Arbeitsspeichers (RAM), der auf dem Endpunkt installiert oder zugeordnet ist.
Typ	X86-basierter PC	Der Prozessortyp des Endpunkts.
Windows Benutzername	TREND-4136D2DB3\admin	Der Benutzername des Windows-Kontos, das sich das letzte Mal am Endpunkt angemeldet hat.

Gerät auslöschen

Die Ausführung eines „Auslöschen"-Befehls löscht alle Endpoint Encryption Gerätedaten. Welche Daten gelöscht werden, ist abhängig vom Geltungsbereich der Daten, der vom verbundenen Endpoint Encryption Agent verwaltet wird. Wenn Sie beispielsweise einen „Auslöschen"-Befehl auf ein Full Disk Encryption Gerät ausführen, werden alle Daten vom Endpunkt gelöscht. Führen Sie dagegen einen „Auslöschen"-Befehl auf ein File Encryption Gerät aus, werden alle Dateien und Ordner auf dem lokalen Datenträger und auf den Wechselmedien gelöscht, die vom File Encryption Agent geschützt werden. Der „Auslöschen"-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert.

Warnung!

Das Auslöschen eines Geräts kann nicht rückgängig gemacht werden. Führen Sie eine Datensicherung der gesamten Daten durch, bevor Sie einen Auslöschen-Befehl geben.

Prozedur

1. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf das Gerät in der Tabelle, und wählen Sie **Auslöschen**.
   - Wählen Sie das Gerät in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend **Auslöschen**.

3. Klicken Sie zur Bestätigung auf **Ja**, wenn die Warnmeldung angezeigt wird.

Gerät sperren

Wenn Sie den Befehl „Sperren“ auf das Endpoint Encryption Gerät anwenden, wird der Endpoint Encryption Benutzerzugriff verhindert, bis eine erfolgreiche Authentifizierung für die Remote-Hilfe durchgeführt wurde. Beim Sperren eines Gerät wird der Endpunkt neu gestartet und in einen Status gezwungen, der Remote-Hilfe erfordert. Der Sperren-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert.

Prozedur

1. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf das Gerät in der Tabelle, und wählen Sie **Sperren**.
   - Wählen Sie das Gerät in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend **Sperren**.

3. Klicken Sie zur Bestätigung auf **Ja**, wenn die Warnmeldung angezeigt wird.

Ein Gerät zurücksetzen

Wenn Sie einen „Warmstart"-Befehl geben, wird der Endpunkt neu gestartet. Der Befehl wird das nächste Mal ausgeführt, wenn der Agent mit PolicyServer kommuniziert.

Prozedur

1. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

2. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf das Gerät in der Tabelle, und wählen Sie **Warmstart**
   - Wählen Sie das Gerät in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend **Warmstart**

3. Klicken Sie zur Bestätigung auf **Ja**, wenn die Warnmeldung angezeigt wird.

Gerät aus dem Unternehmen löschen

Wenn Sie ein Endpoint Encryption Gerät aus dem Unternehmen löschen, wird das Gerät auch aus allen Richtliniengruppen entfernt. Das gelöschte Endpoint Encryption Gerät funktioniert, solange die Richtlinien für Konnektivität und Kennwort auf dem Gerät aktuell sind. Die Endpoint Encryption Benutzer können jedoch keine Dateien wiederherstellen, wenn es auf dem Endpoint Encryption Gerät zu einem kritischen Hardwarefehler kommt, nachdem es aus dem Unternehmen entfernt wurde. Um das Risiko zu senken, sollten Sie das Endpoint Encryption Gerät sofort entschlüsseln und die Software für den Endpoint Encryption Agent deinstallieren.

Informationen zum Entfernen eines Geräts aus einer bestimmten Richtlinie, aber nicht aus dem Unternehmen finden Sie unter *Gerät aus einer Richtlinie entfernen auf Seite 7-6*.

Warnung!

Sorgen Sie dafür, dass das Gerät (Dateien oder Festplatte) entschlüsselt wird, und deinstallieren Sie den Endpoint Encryption Agent, bevor Sie ein Gerät aus dem Unternehmen löschen. Andernfalls besteht die Gefahr von Datenverlusten.

Prozedur

1. Deinstallieren Sie den Endpoint Encryption Agent vom Endpunkt.

   Hinweis

   Informationen zur Deinstallation von Endpoint Encryption Agents finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

2. Suchen Sie das Gerät.

   Siehe *Ein Gerät suchen auf Seite 7-9*.

3. Wählen Sie eine der folgenden Optionen:

   - Klicken Sie mit der rechten Maustaste auf das Gerät in der Tabelle, und wählen Sie **Gerät löschen**
   - Wählen Sie das Gerät in der Tabelle, klicken Sie auf das -Symbol, und wählen Sie anschließend **Gerät löschen**

4. Klicken Sie zur Bestätigung auf **Ja**, wenn die Warnmeldung angezeigt wird.

Das Endpoint Encryption Gerät wird aus dem Unternehmen gelöscht.

Hinweis

Informationen darüber, wie Sie das Endpoint Encryption Gerät wieder dem Unternehmen hinzufügen, finden Sie unter *Gelöschtes Gerät wiederherstellen auf Seite 7-19*.

Gelöschtes Gerät wiederherstellen

Im Umgebungen mit Control Manager und PolicyServer MMC können Sie gelöschte Endpoint Encryption Geräte mit dem Papierkorb-Knoten von PolicyServer MMC wiederherstellen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.
3. Erweitern Sie den **Papierkorb**.
4. Öffnen Sie **Gelöschte Geräte**.

   Im rechten Fensterbereich werden alle gelöschten Endpoint Encryption Geräte angezeigt.
5. Klicken Sie mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie anschließend **Gerät wiederherstellen**.

   Das Endpoint Encryption Gerät wird wieder zum Unternehmen hinzugefügt, gehört jedoch keiner Richtliniengruppe an.

Teil III

Administration mit Endpoint Encryption PolicyServer MMC

Kapitel 8

Erste Schritte mit PolicyServer MMC

Vor der Konfiguration von PolicyServer MMC zur Verwaltung von PolicyServer vergewissern Sie sich, dass PolicyServer Dienste und Datenbanken installiert und konfiguriert wurden.

Hinweis

Informationen zur Installation und Konfiguration von PolicyServer MMC finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*, das Sie unter folgender Adresse finden:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

---

Es werden folgende Themen behandelt:

- *Info über PolicyServer MMC auf Seite 8-2*
- *Bei PolicyServer MMC anmelden auf Seite 8-2*
- *PolicyServer MMC-Benutzeroberfläche auf Seite 8-4*
- *Mit Gruppen und Benutzern arbeiten auf Seite 8-6*
- *Richtliniensteuerelemente verstehen auf Seite 8-16*
- *Agents deaktivieren auf Seite 8-21*

Info über PolicyServer MMC

Das Plug-in PolicyServer Microsoft Management Console (PolicyServer MMC) ist die native Management-Konsole zur Verwaltung von Richtlinien, Benutzern und Geräten für Endpoint Encryption.

Sie können Endpoint Encryption nur mit PolicyServer MMC flexibel verwalten, oder Sie verwalten Endpoint Encryption mit Control Manager für die Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

Sie können mit PolicyServer MMC Folgendes zentral verwalten:

- Alle Benutzer, Geräte und Gruppen von Endpoint Encryption
- Alle Verschlüsselungs-, Kennwortkomplexitäts- und Authentifizierungsrichtlinien
- Remote-Aktionen zur Gerätemanipulation, inkl. Auslöschen eines Geräts, Löschen von Daten oder Verzögern der Authentifizierung
- Ereignisprotokolle über Authentifizierungsereignisse, Verwaltungsereignisse und Sicherheitsverstöße sowie den Geräteverschlüsselungsstatus
- Remote-Hilfe zum Zurücksetzen des Kennworts
- Optionen für Audits und Berichterstellung

Bei PolicyServer MMC anmelden

Sie können den Namen des Unternehmens und das Unternehmensadministratorkonto während der Installation von PolicyServer konfigurieren. Informationen über die kostenlose Testlizenz für 30 Tage finden Sie unter *Testlizenz auf Seite 17-3*.

Prozedur

1. Gehen Sie wie folgt vor, um PolicyServer MMC zu öffnen:
   - Doppelklicken Sie auf dem Desktop auf die Verknüpfung **PolicyServer MMC**.

- Wechseln Sie in den Ordner, der während der Installation festgelegt wurde, und doppelklicken Sie anschließend auf `PolicyServerMMC.exe`.

Das Authentifizierungsfenster für PolicyServer MMC wird angezeigt.

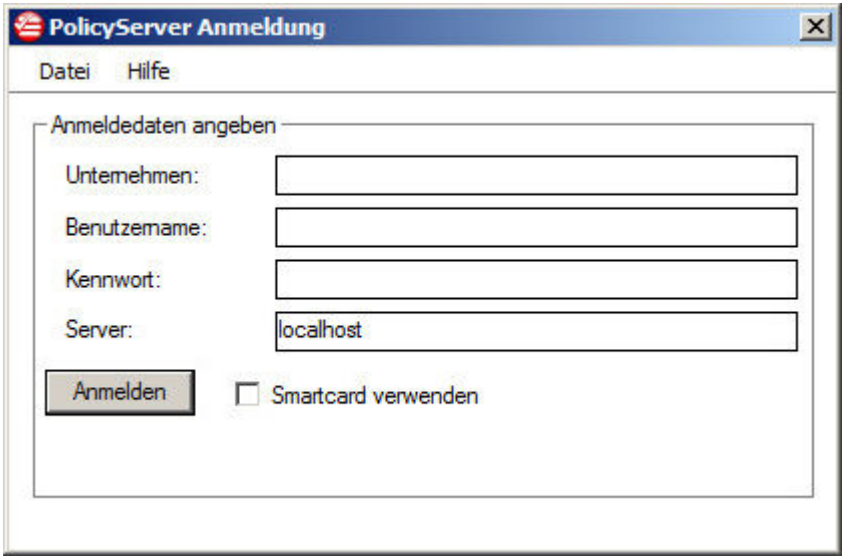


ABBILDUNG 8-1. Das Authentifizierungsfenster von PolicyServer MMC

2. Geben Sie die folgenden Parameter an:

OPTION	BEZEICHNUNG
Unternehmen	Geben Sie das Unternehmen ein.
Benutzername	Geben Sie den Benutzernamen eines Unternehmensadministratorkontos ein.
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.
Server	Geben Sie die IP-Adresse oder den Host-Namen von PolicyServer einschließlich der Portnummer ein, die dieser Konfiguration zugeordnet wurde.

3. Optional: Wenn eine Smartcard zur Authentifizierung verwendet werden soll, wählen Sie **Smartcard verwenden**.

4. Klicken Sie auf **Anmelden**.

5. Warten Sie, bis PolicyServer MMC eine Verbindung zu PolicyServer erstellt.

PolicyServer MMC wird geöffnet.

PolicyServer MMC-Benutzeroberfläche

Die Benutzeroberfläche von PolicyServer MMC besteht aus den folgenden Fensterbereichen:

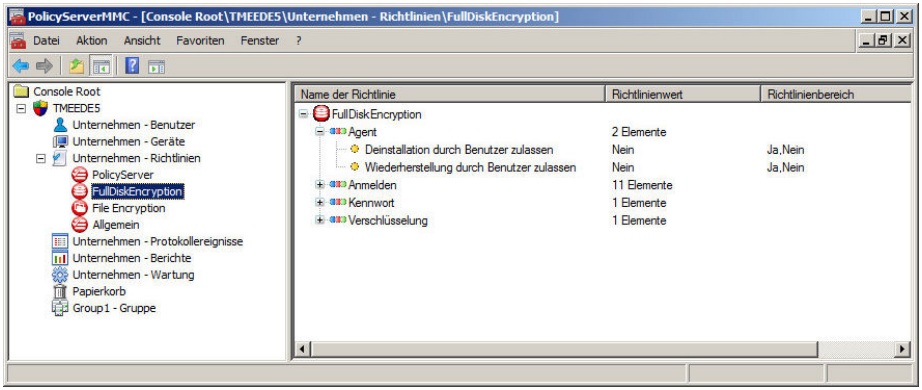


ABBILDUNG 8-2. POLICYSERVER MMC-BENUTZEROBERFLÄCHE

TABELLE 8-1. BESCHREIBUNG DER BENUTZEROBERFLÄCHE VON POLICYSERVER MMC

FENSTERBEREICH	BESCHREIBUNG
Links (1)	Im linken Fensterbereich können Sie Benutzer, Gruppen, Richtlinien, Geräte und Agents anzeigen. Erweitern Sie einen Knoten, um verschachtelte Elemente innerhalb der Baumstruktur zu verwalten. Wenn Sie ein Element öffnen, wird der Inhalt im rechten Fensterbereich entsprechend aktualisiert.

Fensterbereich	Beschreibung
Rechts (2)	Im rechten Fensterbereich ändern Sie Richtlinien, aktualisieren Benutzer- und Gruppeninformationen, zeigen Berichte an und pflegen andere Funktionen. Das genaue Format der im rechten Fensterbereich angezeigten Informationen hängt vom linken Fensterbereich ab.

Die Baumstruktur im linken Fensterbereich umfasst eine Reihe unterschiedlicher Knoten. In der folgenden Tabelle werden die einzelnen Knoten beschrieben:

Tabelle 8-2. Beschreibung der Struktur von PolicyServer MMC

Knoten	Beschreibung
Unternehmen - Benutzer	Sie können alle Administrator- und Benutzerkonten innerhalb des Unternehmens anzeigen. Wenn Sie die Gruppenzugehörigkeit anzeigen möchten, öffnen Sie die Gruppe, und klicken Sie dann auf **Benutzer**.
Unternehmen - Geräte	Sie können alle Instanzen der Endpoint Encryption Agents anzeigen. Außerdem können Sie anzeigen, von welchem Endpoint Encryption Gerät aus die Verbindung hergestellt wurde. Wenn Sie die Gruppenzugehörigkeit anzeigen möchten, öffnen Sie die Gruppe, und klicken Sie dann auf **Geräte**.
Unternehmen - Richtlinien	Mit diesem Knoten steuern Sie, ob Agents eine Verbindung zu PolicyServer herstellen können. Außerdem können Sie alle Unternehmensrichtlinien verwalten. Gruppenrichtlinien setzen Unternehmensrichtlinien außer Kraft.
Unternehmen - Protokollereignisse	Zeigen Sie alle Protokolleinträge für das Unternehmen an.
Unternehmen - Berichte	Verwalten Sie die verschiedenen Berichte und Warnungen. Berichte nur für Gruppen sind nicht verfügbar.
Unternehmen - Wartung	Sie können Anwendungs-Plug-ins von PolicyServer MMC verwalten.
Papierkorb	Sie können gelöschte Endpoint Encryption Benutzer und Geräte anzeigen.

KNOTEN	BESCHREIBUNG
Gruppen	Sie können Endpoint Encryption Benutzer, Gruppen, Richtlinien und Protokollereignisse für eine Auswahl von Benutzern verwalten.

Mit Gruppen und Benutzern arbeiten

In diesem Abschnitt wird der Einstieg in Gruppen und Benutzer in PolicyServer MMC erläutert. Definieren Sie zunächst die Benutzer und Gruppen und weisen Sie die Benutzer anschließend den Gruppen zu. Sie können neue Benutzer auch direkt zu einer Gruppe hinzufügen. Es ist mindestens eine Top-Gruppe erforderlich.

Empfehlungen für Benutzer und Gruppen:

- Folgen Sie der Active Directory-Struktur.
- Erstellen Sie eine neue Gruppe, wann immer unterschiedliche Richtlinien zwischen Benutzergruppen bestehen. Wenn z. B. eine Gruppe eine Domänenauthentifizierung und eine andere ein festes Kennwort erfordert, werden zwei separate Gruppen benötigt.
- Sie können mehrere Gruppen erstellen, um den Zugriff zu minimieren. Alle Mitglieder einer Gruppe sind berechtigt, auf alle Endpoint Encryption Geräte in dieser Gruppe zuzugreifen.

Benutzer und Gruppen definieren

Definieren Sie alle Rollen und Gruppenzugehörigkeiten, bevor Sie Benutzer oder Gruppen hinzufügen.

1. Identifizieren Sie Unternehmensadministrator-/Authentifiziererkonten.
2. Erstellen Sie Unternehmensadministrator-/Authentifiziererkonten.
3. Identifizieren Sie Gruppen.
4. Erstellen Sie Gruppen.

5. Identifizieren Sie Gruppenadministrator-/Authentifiziererkonten.
6. Erstellen Sie Gruppenadministrator-/Authentifiziererkonten.
7. Identifizieren Sie die Benutzer, die Sie jeder Gruppe zuweisen.
8. Importieren oder erstellen Sie neue Benutzer für jede Gruppe.

Top-Gruppe hinzufügen

Gruppen vereinfachen die Verwaltung von Endpoint Encryption Agents, Benutzern, Richtlinien, Untergruppen und Geräten. Die Top-Gruppe ist die Gruppe auf der höchsten Stufe.

Hinweis

Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer Gruppen hinzuzufügen. Um einen Gruppenadministrator zu erstellen, fügen Sie einen Benutzer hinzu, und ändern Sie seine Kontoberechtigungen innerhalb der Gruppe. Weitere Informationen finden Sie unter *Benutzer ändern auf Seite 11-9*.

Prozedur

1. Klicken Sie mit der rechten Maustaste im linken Fenster auf das Unternehmen, und klicken Sie anschließend auf **Top-Gruppe hinzufügen**.

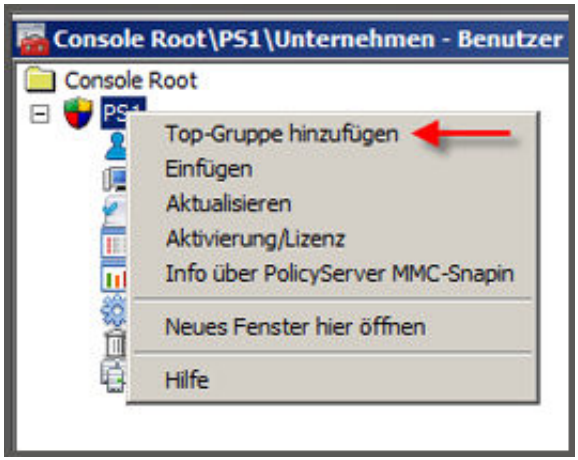


ABBILDUNG 8-3. Fenster "Top-Gruppe hinzufügen"

Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Geben Sie den Namen und eine Beschreibung der Gruppe an.

3. Wenn Endpoint Encryption Geräte verwendet werden, die Unicode nicht unterstützen, wählen Sie **Altgeräte unterstützen**.

Hinweis

Einige Altgeräte sind möglicherweise nicht in der Lage, unter Verwendung von Unicode mit PolicyServer zu kommunizieren. Weisen Sie Unicode-Geräte und ältere Endpoint Encryption Geräte verschiedenen Gruppen zu.

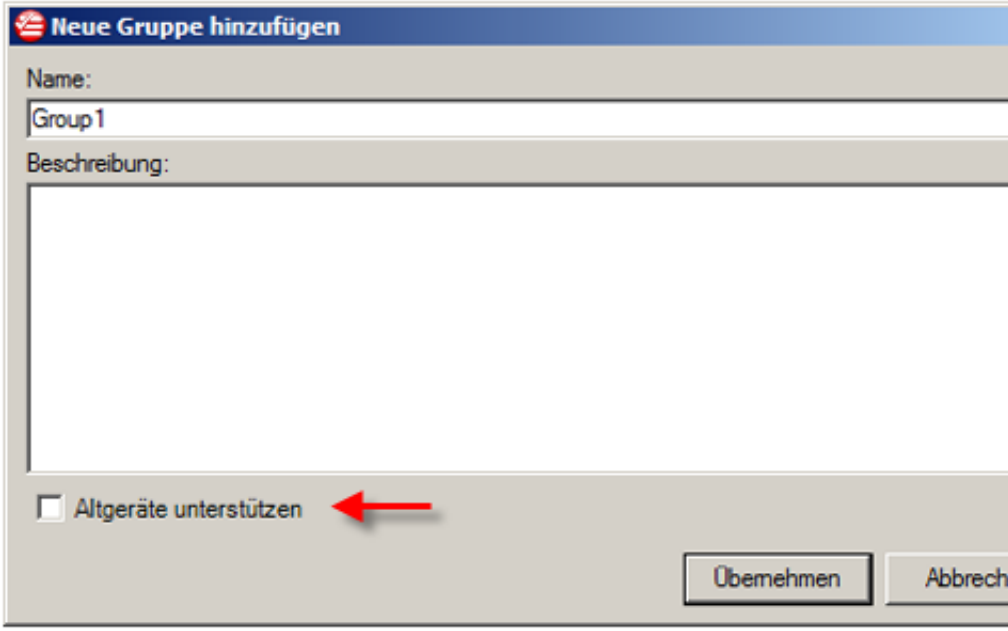


ABBILDUNG 8-4. Fenster "Neue Gruppe hinzufügen"

4. Klicken Sie auf **Übernehmen**.
5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

   Die neue Gruppe wird zur Baumstruktur im linken Fensterbereich hinzugefügt.

Neuen Benutzer zu einer Gruppe hinzufügen

Hinweis

Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.

Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.

2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Neuen Benutzer hinzufügen**.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

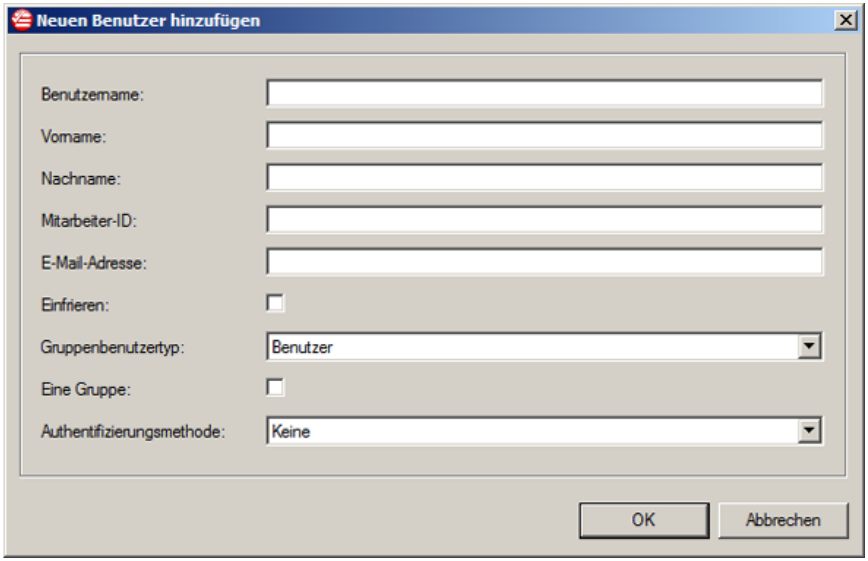


ABBILDUNG 8-5. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die folgenden Optionen an:

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen für das neue Benutzerkonto an (erforderlich).
Vorname	Geben Sie den Vornamen des Benutzers für das neue Benutzerkonto an (erforderlich).

Option	Bezeichnung
Nachname	Geben Sie den Nachnamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers für das neue Benutzerkonto an (optional).
Einfrieren	Wählen Sie, ob das neue Benutzerkonto vorübergehend deaktiviert werden soll (optional). Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräten anmelden.
Gruppenbenutzertyp	Wählen Sie die Berechtigungen für das neue Konto. **Hinweis** Informationen über Kontorollen finden Sie unter *Endpoint Encryption Benutzerrollen auf Seite 2-6*. Zu den Optionen gehören: • Benutzer • Authentifizierer • Administrator **Hinweis** Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer zu Gruppen hinzuzufügen.
Eine Gruppe	Wählen Sie, ob das neue Benutzerkonto ein Mitglied von mehreren Gruppenrichtlinien sein darf.
Authentifizierungsmethode	Wählen Sie die Methode aus, mit der sich das neue Benutzerkonto an den Endpoint Encryption Geräten anmelden wird.

Option	Bezeichnung
	Hinweis Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**. Informationen über Kontorollen finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*.

4. Klicken Sie auf **OK**.

   Der neue Benutzer wird der ausgewählten Gruppe und zum Unternehmen hinzugefügt. Der Benutzer kann sich nun an den Endpoint Encryption Geräten anmelden.

Neuen Unternehmensbenutzer hinzufügen

Das folgende Verfahren erklärt, wie Sie neue Endpoint Encryption Benutzer dem Unternehmen hinzufügen.

Hinweis

Wenn Sie einen neuen Endpoint Encryption Benutzer zum Unternehmen hinzufügen, wird der Benutzer keiner Gruppe zugewiesen.

Beim Hinzufügen eines Endpoint Encryption Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Gehen Sie wie folgt vor, um auf Benutzer im Unternehmen zuzugreifen:
   - Erweitern Sie das Unternehmen, und öffnen Sie anschließend **Unternehmen - Benutzer**.
   - Erweitern Sie das Unternehmen, erweitern Sie die Gruppe, und öffnen Sie anschließend **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf einen leeren Bereich im rechten Fensterbereich, und wählen Sie **Benutzer hinzufügen** aus.

Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

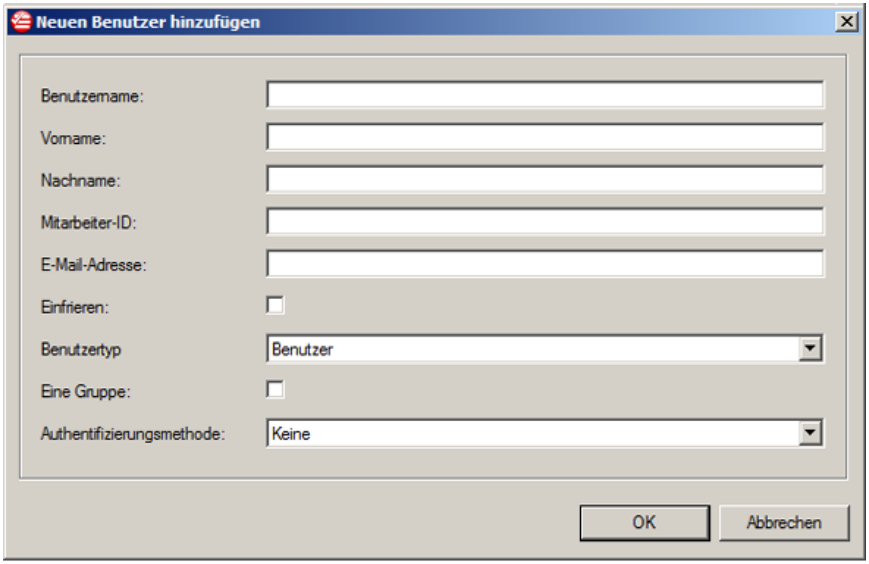


ABBILDUNG 8-6. FENSTER "NEUEN BENUTZER HINZUFÜGEN"

3. Geben Sie die folgenden Optionen an:

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen für das neue Benutzerkonto an (erforderlich).
Vorname	Geben Sie den Vornamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Nachname	Geben Sie den Nachnamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers für das neue Benutzerkonto an (optional).
Einfrieren	Wählen Sie, ob das neue Benutzerkonto vorübergehend deaktiviert werden soll (optional).

Option	Bezeichnung
	Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräten anmelden.
Gruppenbenutzertyp	Wählen Sie die Berechtigungen für das neue Konto. Informationen über Kontorollen finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*. Zu den Optionen gehören: • **Benutzer** • **Authentifizierer** • **Administrator** **Hinweis** Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer zu Gruppen hinzuzufügen.
Eine Gruppe	Wählen Sie, ob das neue Benutzerkonto ein Mitglied von mehreren Gruppenrichtlinien sein darf.
Authentifizierungsmethode	Wählen Sie die Methode aus, mit der sich das neue Benutzerkonto an den Endpoint Encryption Geräten anmelden wird. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*. **Hinweis** Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

4. Klicken Sie auf **OK**.

   Der neue Endpoint Encryption Benutzer wird dem Unternehmen hinzugefügt. Der Benutzer kann sich zuerst bei Endpoint Encryption Geräten anmelden, nachdem das Benutzerkonto einer Gruppe hinzugefügt wurde.

Vorhandenen Benutzer zu einer Gruppe hinzufügen

Ein Benutzer kann in mehreren Gruppen Mitglied sein.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster, und klicken Sie auf **Benutzer**.
2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Vorhandenen Benutzer hinzufügen**.

   Das Fenster **Benutzer zu Gruppe hinzufügen** wird angezeigt.

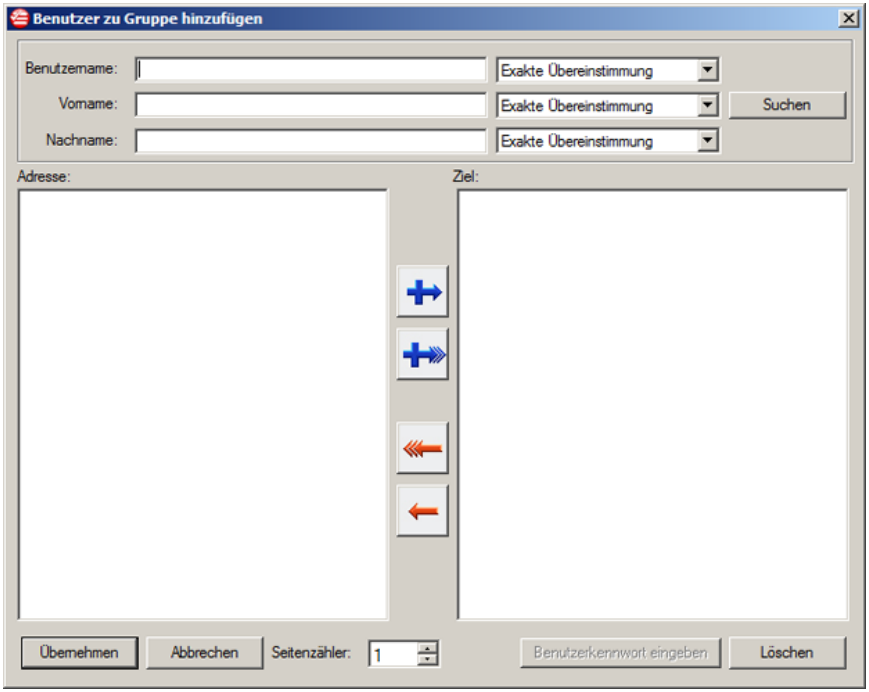


ABBILDUNG 8-7. Fenster "Benutzer zu Gruppe hinzufügen"

3. Geben Sie die Benutzerdetails ein und klicken Sie dann auf **Suchen**.

Im Feld **Quelle** werden die Konten angezeigt, die den Suchkriterien entsprechen.

4. Wählen Sie Benutzer aus der Liste im Feld **Quelle** aus, und klicken Sie auf den blauen Pfeil, um sie hinzufügen.

   Weitere Informationen zu Suchsymbolen finden Sie unter *Symbole für Suchergebnisse hinzufügen/entfernen auf Seite 11-15*.

   Der ausgewählte Benutzer wird in die Liste **Ziel** verschoben.

5. So ändern Sie ein Benutzerkennwort:

   a. Markieren Sie den Benutzer in der Liste **Ziel**.

   b. Klicken Sie im unteren Fensterbereich auf **Benutzerkennwort eingeben**.

   c. Geben Sie im anschließend angezeigten Fenster die Authentifizierungsmethode für den Benutzer an.

   d. Klicken Sie auf **Übernehmen**, um das Fenster **Kennwort ändern** zu schließen.

6. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

   Der Benutzer wird zur Gruppe hinzugefügt. Wenn es sich um die einzige Gruppenzuweisung handelt, kann sich der Benutzer nun bei den Endpoint Encryption Geräten anmelden.

Richtliniensteuerelemente verstehen

Nachdem Sie Benutzer und Gruppen hinzugefügt und konfiguriert haben, legen Sie Richtlinien für das Unternehmen oder die Gruppe fest. Jede Gruppe (ob Top-Gruppe oder Untergruppe) enthält einen „Richtlinien“-Knoten mit speziellen Richtlinien für den jeweiligen Agent und anderen allgemeinen Richtlinien, die sich auf alle Agents und die Authentifizierung auswirken.

Hinweis

Informationen zur Deaktivierung oder Aktivierung von Richtlinien auf Unternehmens- oder Gruppenebene finden Sie unter *Auf Richtlinien zugreifen auf Seite 9-4*.

Weitere Informationen zur Benutzeroberfläche von PolicyServer MMC finden Sie unter *PolicyServer MMC-Benutzeroberfläche auf Seite 8-4*.

Optische Indikatoren für Richtlinien

Die kleinen farbigen Kreise links neben jeder Richtlinie geben einen der folgenden Statuswerte an:

- Richtlinienstufe
- Modifikationsstatus der Gruppe
- Ein oder mehrere Werte-Arrays
- Ob die Richtlinie Unterrichtlinien enthält

TABELLE 8-3. RICHTLINIENINDIKATOREN

INDIKATOR	BESCHREIBUNG
	Ein einzelner gelber Kreis zeigt an, dass der Richtlinienwert von der übergeordneten Gruppe oder dem Unternehmen übernommen wurde.
	Ein einzelner blauer Kreis zeigt an, dass die Richtlinie für die Gruppe geändert wurde.
	Drei blaue Kreise zeigen an, dass eine Richtlinie möglicherweise mehrere Werte-Arrays enthält.
	Drei mehrfarbige Kreise (rot, blau, grün) zeigen an, dass die Richtlinie mindestens eine Unterrichtlinie hat.

Felder und Schaltflächen für Richtlinien

In der folgenden Tabelle werden die Felder und Schaltflächen beschrieben, die die Richtlinien in PolicyServer MMC steuern. Alle geänderten Werte werden auf die

Untergruppen der jeweiligen Gruppe übertragen. Nur die relevanten Felder und Schaltflächen werden in einer ausgewählten Richtlinie angezeigt.

TABELLE 8-4. Felder und Schaltflächen für Richtlinien

FELD/SCHALTFLÄCHE	BESCHREIBUNG	ÄNDERBAR?
OK	Speichert Änderungen in der ausgewählten Richtlinie.	n. v.
Beschreibung	Beschreibt die ausgewählte Richtlinie.	Nein
Richtlinienbereich	Zeigt den zulässigen Wertebereich für die ausgewählte Richtlinie an.	Ja
Richtlinienwert	Zeigt abhängig von der Richtlinie den aktuellen Wert der ausgewählten Richtlinie an (ob eine Zeichenfolge, eine Zahl oder eine Serie von Einträgen enthalten ist).	Ja
Richtlinienmehrfachwert	Gibt an, ob diese Richtlinie mehrere Male für verschiedene Einstellungen verwendet werden kann (z. B. mehrere "Falls gefunden"-Zeichenfolgen).	Nein
Name der Richtlinie	Zeigt den Namen der ausgewählten Richtlinie an.	Nein
Richtlinientyp	Gibt die Kategorie der ausgewählten Richtlinie an.	Nein
Unternehmensgesteuert	Änderungen an dieser Richtlinie werden auf dieselbe Richtlinie auf Unternehmensebene gespiegelt.	Ja
In Untergruppen speichern	Verteilt die Richtlinieneinstellungen auf dieselben Richtlinien in allen Untergruppen.	Ja

Richtlinien ändern

PolicyServer MMC verfügt über mehrere allgemeine Fenster zum Ändern von Richtlinien. Je nachdem, welche Elemente die Richtlinie steuert und welche Parameter erforderlich sind, stehen unterschiedliche Arten der Eingabe zur Verfügung. Mit dieser Aufgabe wird ein allgemeiner Überblick über die Bearbeitung einer Richtlinie

bereitgestellt. Die Bearbeitung verschiedener Richtlinien erfordert auch unterschiedliche Schritte.

Hinweis

Weitere Informationen zur Bearbeitung von Richtlinien, einschließlich Erläuterungen zur Konfiguration unterschiedlicher Richtlinientypen, finden Sie unter *Auf Richtlinien zugreifen auf Seite 9-4*.

Prozedur

1. Erweitern Sie den Knoten **Unternehmen**.
2. Wählen Sie die Richtlinienebene aus, die geändert werden soll.
   - Für Unternehmensrichtlinien erweitern Sie **Unternehmen - Richtlinien**.
   - Für Gruppenrichtlinien erweitern Sie den **Gruppennamen** und anschließend **Richtlinien**.
3. Öffnen Sie die spezifische Anwendung oder wählen Sie **Allgemein** aus.

   Die Liste der Richtlinien wird im Ergebnisfenster angezeigt.

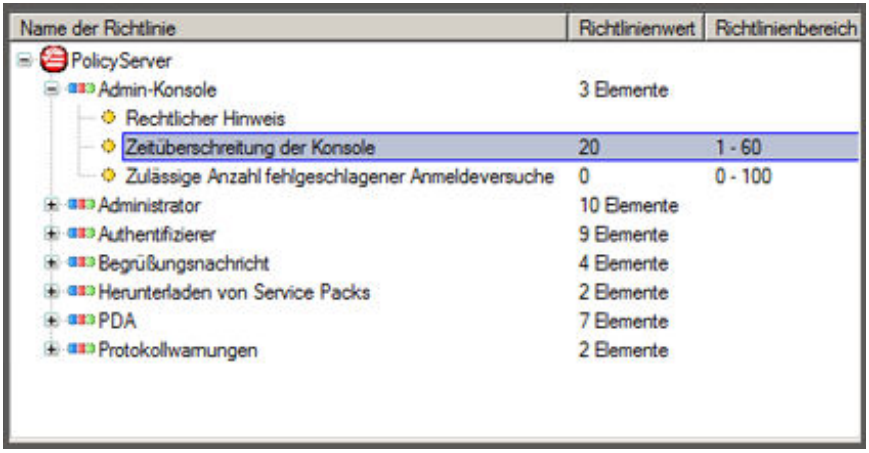


ABBILDUNG 8-8. Ändern einer Richtlinie

4. Navigieren Sie zu einer Richtlinie und doppelklicken Sie darauf, um das Editorfenster zu öffnen.

   Hier als Beispiel die Richtlinie „Zeitüberschreitung der Konsole“:

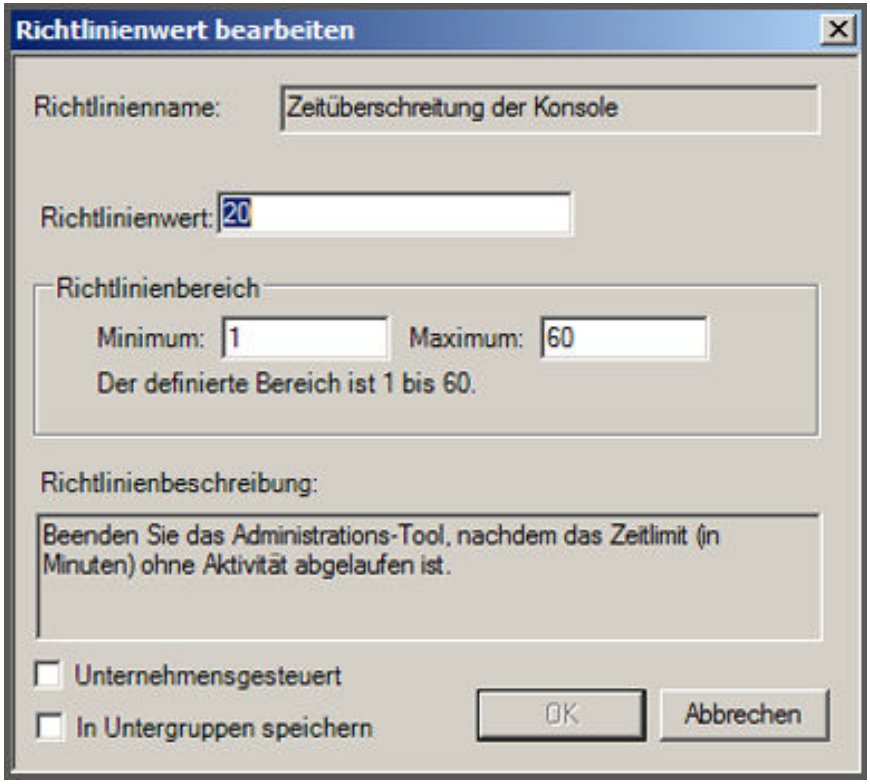


ABBILDUNG 8-9. Editorfenster für die Richtlinie „Zeitüberschreitung der Konsole“

5. Nehmen Sie die für die Richtlinie entsprechenden Änderungen vor, und klicken Sie anschließend auf **OK**.

Agents deaktivieren

Alle Endpoint Encryption Agents sind standardmäßig aktiviert.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.

   Weitere Informationen finden Sie unter *Bei PolicyServer MMC anmelden auf Seite 8-2*.

2. Wählen Sie eine der folgenden Optionen:

   - Um den Agent innerhalb des Unternehmens zu deaktivieren, klicken Sie auf **Unternehmen - Richtlinien**.
   - Um den Agent nur für die Benutzer in der Gruppe zu deaktivieren, erweitern Sie die Gruppe, und klicken Sie anschließend auf **Richtlinien**.

   Alle Anwendungen werden im rechten Fensterbereich angezeigt.

3. Klicken Sie mit der rechten Maustaste auf die Anwendung, und wählen Sie anschließend **Deaktivieren**.

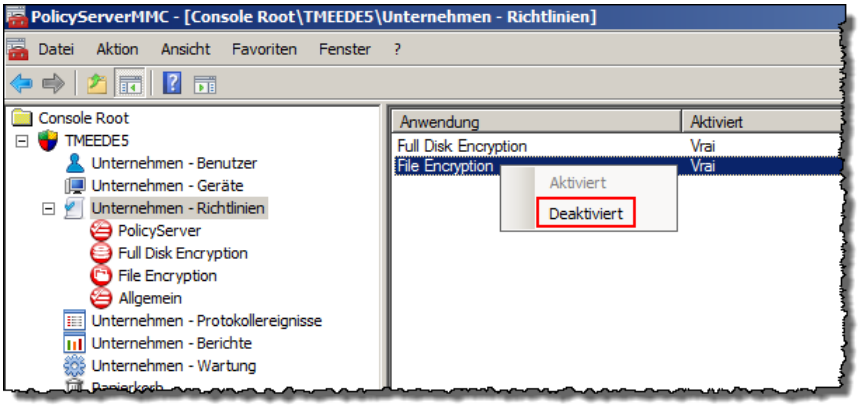


ABBILDUNG 8-10. Agents aktivieren/deaktivieren

Der Endpoint Encryption Agent wird deaktiviert. Endpoint Encryption Benutzer können Sie mit diesem Agent nicht an Geräten anmelden.

Kapitel 9

Richtlinien in PolicyServer MMC

In diesem Kapitel wird erklärt, wie Sie Endpoint Encryption Richtlinien mit PolicyServer MMC verwalten und konfigurieren.

Hinweis

Informationen zur Richtlinienzuordnung zwischen PolicyServer MMC und Control Manager finden Sie unter *Richtlinienzuordnung zwischen Management-Konsolen auf Seite D-1*.

Es werden folgende Themen behandelt:

- *Richtlinienübersicht auf Seite 9-2*
- *Richtlinienzuordnung zwischen Management-Konsolen auf Seite D-1*
- *Automatische Synchronisierung von Richtlinien auf Seite 9-15*
- *PolicyServer Richtlinien auf Seite 9-16*
- *Full Disk Encryption Regeln konfigurieren auf Seite 3-18*
- *File Encryption Regeln konfigurieren auf Seite 3-20*
- *Allgemeine Richtlinien auf Seite 9-33*

Richtlinienübersicht

In diesem Abschnitt wird erläutert, wie verschiedene Fenster zum Ändern einer Richtlinie verwendet werden können. Das Verfahren zum Ändern aller Richtlinien wird hier jedoch nicht erläutert. Die PolicyServer MMC verfügt über einen allgemeinen Satz an Fenstern, die zum Ändern einer Richtlinie verwendet werden können. Die eine Richtlinie weist möglicherweise ein Editorfenster auf, in dem mit der Richtlinie verbundene Zahlen, Bereiche und Werte geändert werden können, während eine andere Richtlinie über ein Fenster zum Ändern von Textzeichenfolgen verfügen kann.

Beachten Sie beim Verwalten von Richtlinien Folgendes:

- Richtlinien können auf Basis des Agent in jeder Gruppe konfiguriert werden.
- Richtlinienvererbung findet nur statt, wenn eine Untergruppe vorhanden ist. Weitere Informationen zu Gruppenberechtigungen finden Sie unter *Info über Gruppen auf Seite 10-2*.
- Jede Richtlinie hat einen Standardwert.

Optische Indikatoren für Richtlinien

Die kleinen farbigen Kreise links neben jeder Richtlinie geben einen der folgenden Statuswerte an:

- Richtlinienstufe
- Modifikationsstatus der Gruppe
- Ein oder mehrere Werte-Arrays
- Ob die Richtlinie Unterrichtlinien enthält

TABELLE 9-1. Richtlinienindikatoren

INDIKATOR	BESCHREIBUNG
	Ein einzelner gelber Kreis zeigt an, dass der Richtlinienwert von der übergeordneten Gruppe oder dem Unternehmen übernommen wurde.

Indikator	Beschreibung
	Ein einzelner blauer Kreis zeigt an, dass die Richtlinie für die Gruppe geändert wurde.
	Drei blaue Kreise zeigen an, dass eine Richtlinie möglicherweise mehrere Werte-Arrays enthält.
	Drei mehrfarbige Kreise (rot, blau, grün) zeigen an, dass die Richtlinie mindestens eine Unterrichtlinie hat.

Felder und Schaltflächen für Richtlinien

In der folgenden Tabelle werden die Felder und Schaltflächen beschrieben, die die Richtlinien in PolicyServer MMC steuern. Alle geänderten Werte werden auf die Untergruppen der jeweiligen Gruppe übertragen. Nur die relevanten Felder und Schaltflächen werden in einer ausgewählten Richtlinie angezeigt.

Tabelle 9-2. Felder und Schaltflächen für Richtlinien

Feld/Schaltfläche	Beschreibung	Änderbar?
OK	Speichert Änderungen in der ausgewählten Richtlinie.	n. v.
Beschreibung	Beschreibt die ausgewählte Richtlinie.	Nein
Richtlinienbereich	Zeigt den zulässigen Wertebereich für die ausgewählte Richtlinie an.	Ja
Richtlinienwert	Zeigt abhängig von der Richtlinie den aktuellen Wert der ausgewählten Richtlinie an (ob eine Zeichenfolge, eine Zahl oder eine Serie von Einträgen enthalten ist).	Ja
Richtlinienmehrfachwert	Gibt an, ob diese Richtlinie mehrere Male für verschiedene Einstellungen verwendet werden kann (z. B. mehrere "Falls gefunden"-Zeichenfolgen).	Nein
Name der Richtlinie	Zeigt den Namen der ausgewählten Richtlinie an.	Nein

FELD/SCHALTFLÄCHE	BESCHREIBUNG	ÄNDERBAR?
Richtlinientyp	Gibt die Kategorie der ausgewählten Richtlinie an.	Nein
Unternehmensgesteuert	Änderungen an dieser Richtlinie werden auf dieselbe Richtlinie auf Unternehmensebene gespiegelt.	Ja
In Untergruppen speichern	Verteilt die Richtlinieneinstellungen auf dieselben Richtlinien in allen Untergruppen.	Ja

Auf Richtlinien zugreifen

Jede Gruppe in PolicyServer MMC enthält mindestens einen Richtlinienordner. Im rechten Fensterbereich wird das Ergebnisfenster angezeigt, das die folgenden Steuerelemente enthält:

- Anzeigen einer Liste mit Richtlinien und deren Werte
- Ändern einer Richtlinie mit dem Editor-Fenster
- Ausführen von Berichten und anderen Protokollereignissen
- Ausführen von Unternehmenswartung

Hinweis

Weitere Informationen zur Benutzeroberfläche von PolicyServer MMC finden Sie unter *PolicyServer MMC-Benutzeroberfläche auf Seite 8-4*.

Richtlinie für Änderung auswählen

Prozedur

1. Navigieren Sie zu **Gruppenname** > **Richtlinien**, und wählen Sie den entsprechenden Knoten.

   Beispiel: **Gruppe1** > **Richtlinien** > **Full Disk Encryption**.

2. Navigieren Sie zur spezifischen Richtlinie.

   Beispiel: **Allgemein** > **Client** > **Deinstallation durch Benutzer zulassen**.

3. Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Eigenschaften** aus.

Richtlinien mit Bereichen bearbeiten

Einige Richtlinien verfügen über Steuerelemente, um einen Wertebereich für die Richtlinienwerte festzulegen, z. B. die minimale und maximale Länge für Kennwörter.

Ein Beispiel für die Bearbeitung von Richtlinien mit Bereichen stellt die Richtlinie **Zulässige Anzahl fehlgeschlagener Anmeldeversuche** dar. **Zulässige Anzahl**

fehlgeschlagener Anmeldeversuche steuert, ob ein Gerät gesperrt wird, wenn ein Benutzer die Anzahl der zulässigen Authentifizierungsversuche überschreitet.

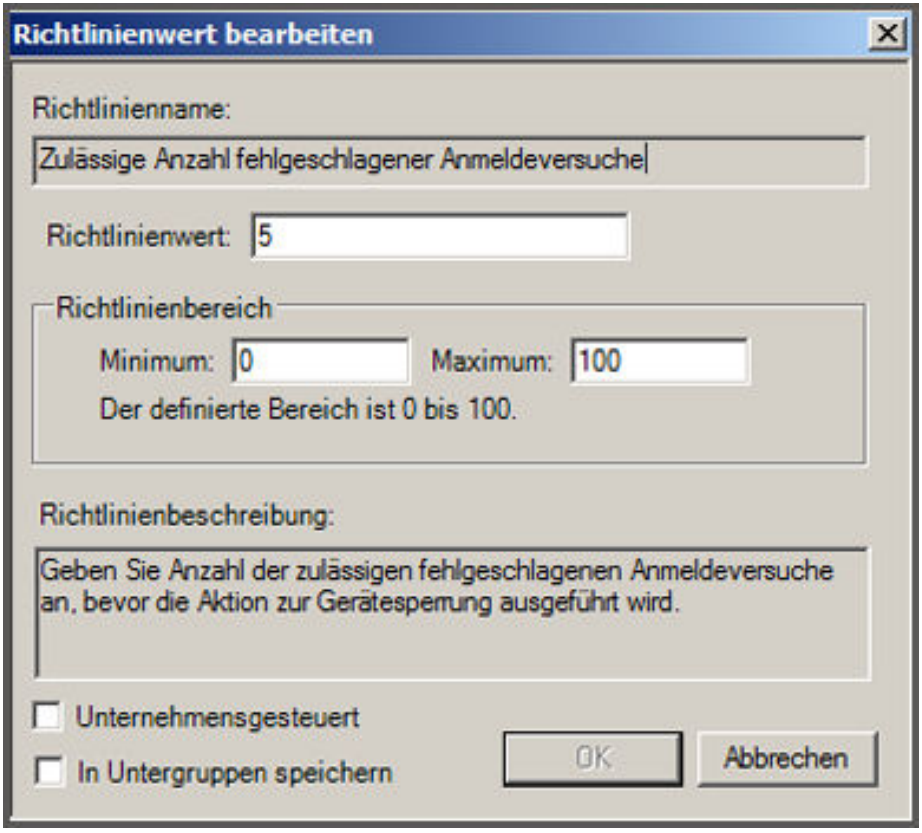


ABBILDUNG 9-1. Fenster "Richtlinie mit Bereichen"

Unter Verwendung der in den Feldern **Richtlinienbereich** definierten Parametern können Sie die Anzahl der fehlgeschlagenen Anmeldeversuche pro Benutzer im Feld **Richtlinienwert** angeben.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.
2. Geben Sie im Feld **Mindestwert** die niedrigste Anzahl von erfolglosen Authentifizierungsversuchen ein, die ein Benutzer in dieser Gruppe tätigen darf, bevor das Gerät gesperrt wird.

   Hinweis

   Die Mindest- und Höchstwerte für den Richtlinienbereich können dem übergeordneten Bereich entsprechen oder durch Eingabe von eindeutigen Werten geändert werden. Es ist nicht möglich, die Mindest- und Höchstwerte zu überschreiten.

3. Geben Sie im Feld **Höchstwert** die höchste Zahl der Authentifizierungsversuche an, die von einem Benutzer in dieser Gruppe vorgenommen werden kann, bevor die Authentifizierung fehlschlägt und das Gerät gesperrt wird.
4. Geben Sie im Feld **Richtlinienwert** die Zahl der fehlgeschlagenen Authentifizierungsversuche an, die von einem Benutzer in dieser Gruppe vorgenommen werden können, bevor das Gerät gesperrt wird.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

   Die Richtlinienänderung wird aktiviert, wenn der Endpoint Encryption Agent mit PolicyServer synchronisiert wird.

Richtlinien mit den Antworten "Wahr/Falsch" oder "Ja/Nein"

Einige Richtlinien weisen nur die Option "Wahr/Falsch" oder "Ja/Nein" auf. Für dieses Beispiel wird **Preboot-Umgehung** verwendet.

Ein Gruppenadministrator kann definieren, ob Full Disk Encryption Preboot vor dem Starten von Windows angezeigt wird. Wenn laut der übergeordneten Gruppe **Ja** und **Nein** zulässig sind, haben die Gruppenauthentifizierer der Untergruppe das Recht, die Einstellung auf **Ja** und **Nein**, nur **Ja** oder nur **Nein** zu ändern. Wenn für die

übergeordnete Gruppe als Einstellung entweder **Ja** oder **Nein** festgelegt wurde, können die Gruppenauthentifizierer der Untergruppe nur dieselbe Einstellung wählen.

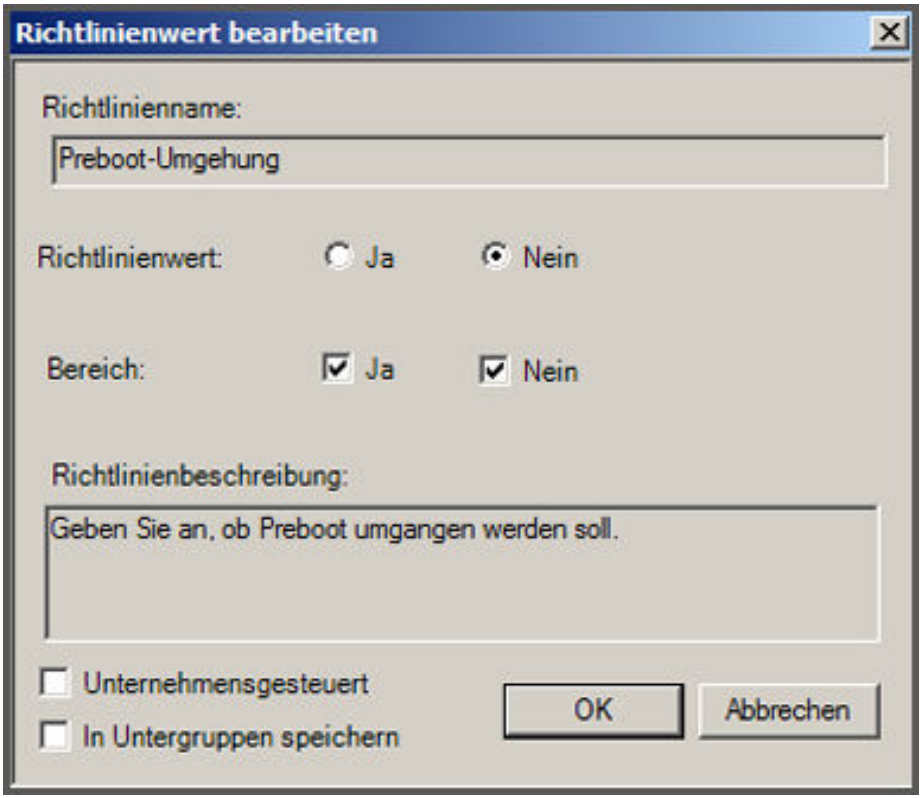


ABBILDUNG 9-2. Richtlinie mit den Werten "Ja/Nein"

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.
2. Geben Sie Richtlinienoptionen an.
   - Mit dem Feld **Richtlinienwert** wird festgelegt, ob die Richtlinie aktiviert wird.

- Mit dem Feld **Bereich** wird festgelegt, ob die Richtlinie anderen Benutzern oder Gruppen zur Verfügung steht.

  Beispiel: Wenn für die Richtlinie **Nein** festgelegt wird, kann für die Richtlinie nicht mehr **Ja** festgelegt werden.

Hinweis

Wenn Sie eine Option aus dem **Richtlinienbereich** entfernen, wird der Wert aus dem Listenfeld **Richtlinienwert** in der aktuellen Gruppe und allen Untergruppen entfernt.

3. Klicken Sie zum Speichern der Änderungen auf **OK**.

   Die Richtlinienänderung wird aktiviert, wenn der Endpoint Encryption Agent mit PolicyServer synchronisiert wird.

Richtlinien mit Mehrfach-/Einfachauswahl bearbeiten

Einige Richtlinien haben mehrere Optionen, die ausgewählt werden können. Die Richtlinie **Aktion zur Gerätesperrung** wird in einem Mehrfach-/Einfachauswahlfenster bearbeitet. Sie können nur einen **Richtlinienwert** auswählen. In diesem Beispiel muss der Gruppenadministrator die durchzuführende Aktion

auswählen, wenn ein Benutzer die zulässige Anzahl an Authentifizierungsversuchen überschreitet.

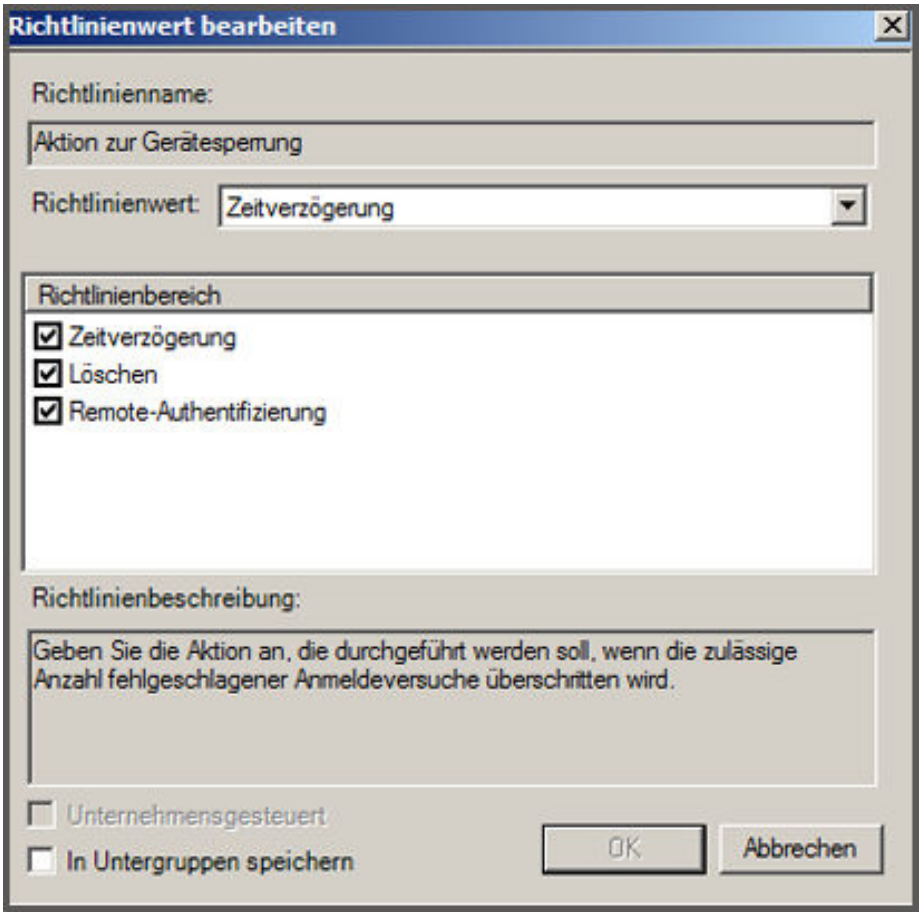


ABBILDUNG 9-3. Richtlinien mit Mehrfach-/Einfachauswahl

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.

2. Wählen Sie eine Standardeinstellung für das Listenfeld **Richtlinienwert** aus.
3. Wählen Sie die verfügbaren Optionen für den Bereich **Richtlinienbereich** aus.

Hinweis

Wenn Sie eine Option aus dem **Richtlinienbereich** entfernen, wird der Wert aus dem Listenfeld **Richtlinienwert** in der aktuellen Gruppe und allen Untergruppen entfernt.

4. Klicken Sie zum Speichern der Änderungen auf **OK**.

   Die Richtlinienänderung wird aktiviert, wenn der Endpoint Encryption Agent mit PolicyServer synchronisiert wird.

Richtlinien mit Textzeichenfolgenargumenten bearbeiten

Einige Richtlinien weisen eine editierbare Textzeichenfolge für einzelne Array-Argumente auf. Die Richtlinie **Kennwort zur Auslöschung** ist ein Beispiel einer Richtlinie, die die Funktion zur Angabe einer Textzeichenfolge bietet.

ABBILDUNG 9-4. Richtlinie mit Textzeichenfolgenargument

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.
2. Geben Sie die Zeichenfolge für diese Richtlinie in das Feld **Richtlinienwert** ein.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

   Die Richtlinienänderung wird aktiviert, wenn der Endpoint Encryption Agent mit PolicyServer synchronisiert wird.

Richtlinien mit mehreren Optionen bearbeiten

Einige Richtlinien können über mehrere in Unterrichtlinien gespeicherten Optionen verfügen, die sich auf diese Richtlinie auswirken. Mehrere Optionsrichtlinien erstellen getrennte Zeilen in einer Textzeichenfolge, wobei jede neue Zeile in der Zeichenfolge eine Unterrichtlinie darstellt. Beispiel: Die Richtlinie **Falls gefunden** zeigt an, wie ein gefundenes Gerät zurückgegeben wird. Ein normales Adressformat zeigt den Namen, die Straße sowie Stadt/Bundesland/Postleitzahl in drei getrennten Zeilen an.

Hinweis

Abhängig von der Richtlinie sind Mehrfachoptionen generell auf sechs Unterrichtlinien begrenzt.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie, und klicken Sie dann auf **Hinzufügen**.

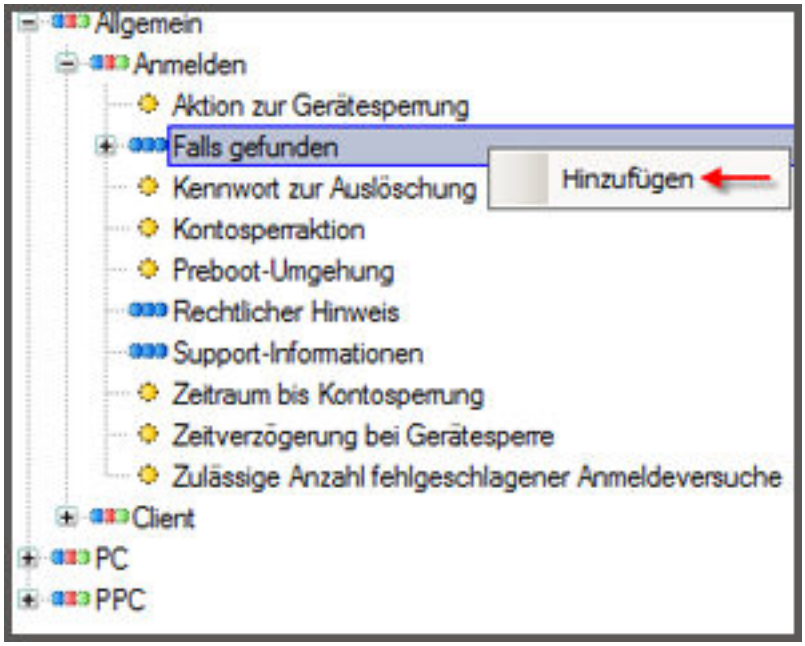


ABBILDUNG 9-5. Falls gefunden-Richtlinie: Neue Option hinzufügen

2. Geben Sie die Details in das Feld **Richtlinienwert** ein.

Hinweis

Abhängig von der Richtlinie müssen Sie möglicherweise die hinzugefügte Richtlinie ändern, indem Sie mit der rechten Maustaste darauf klicken und **Eigenschaften** auswählen.

---

3. Klicken Sie zum Speichern der Änderungen auf **OK**.

Falls gefunden	3 Elemente	
Falls gefunden	Name	255 Zeichen
Falls gefunden	Steet Address	255 Zeichen
Falls gefunden	City / State / Zip Code	255 Zeichen

ABBILDUNG 9-6. Falls gefunden-Richtlinie: Ergebnisse nach dem Hinzufügen mehrerer Optionen

4. Fügen Sie bei Bedarf eine neue Option hinzu.

5. Um Änderungen vorzunehmen, klicken Sie mit der rechten Maustaste auf die untergeordnete Richtlinie, und wählen Sie anschließend **Eigenschaften** aus.

   Die Richtlinienänderung wird aktiviert, wenn der Endpoint Encryption Agent mit PolicyServer synchronisiert wird.

Automatische Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Endpoint Encryption Agents und PolicyServer einleiten.

- Nachdem das Betriebssystem geladen wird und der Dienst des Endpoint Encryption Agent startet

  Hinweis

  Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- Wenn Full Disk Encryption Preboot startet (nur Full Disk Encryption)
- Die Zeitdauer der Richtlinie **Synchronisierungsintervall** läuft ab

Öffnen Sie das Fenster **Info über**, um Endpoint Encryption Agent anzuweisen, die Richtlinien manuell zu synchronisieren.

Hinweis

Aktionen für Endpoint Encryption Geräte werden eingeleitet, nachdem der Endpoint Encryption Agent Richtlinien-Updates erhält.

PolicyServer Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für Richtlinien erläutert, die sich auf PolicyServer auswirken.

Richtlinien für die Admin-Konsole

In der folgenden Tabelle werden die Richtlinien beschrieben, die PolicyServer MMC steuern.

TABELLE 9-3. Beschreibung der Richtlinien für die Admin-Konsole für PolicyServer

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Zeitüberschreitung der Konsole	Beenden Sie das Administrations-Tool, nachdem das Zeitlimit (in Minuten) ohne Aktivität abgelaufen ist.	1-60 Standard: 20
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Admin-Anmeldung nach dieser Anzahl aufeinanderfolgender fehlgeschlagener Anmeldeversuche sperren.	0-100 Standard: 0
Rechtlicher Hinweis	Enthält den rechtlichen Hinweis, der angezeigt werden muss, bevor der Administrator oder Authentifikator die Administrations-Tools verwenden kann.	1-1024 Zeichen Standard: n. v.

Administratorrichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die PolicyServer Berechtigungen für Gruppenadministratoren bestimmen.

Tabelle 9-4. Beschreibung der Administratorrichtlinien für PolicyServer

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Geräte hinzufügen	Geben Sie an, ob der Gruppenadministrator Geräte hinzufügen darf.	Ja, Nein Standard: Ja
Benutzer hinzufügen	Geben Sie an, ob der Gruppenadministrator neue Benutzer hinzufügen darf.	Ja, Nein Standard: Ja
Benutzer zu Unternehmen hinzufügen	Geben Sie an, ob der Gruppenadministrator neue Benutzer zum Unternehmen hinzufügen darf.	Ja, Nein Standard: Nein
Gruppen hinzufügen/ändern	Geben Sie an, ob der Gruppenadministrator Untergruppen hinzufügen/ändern darf.	Ja, Nein Standard: Ja
Richtlinien ändern	Geben Sie an, ob der Gruppenadministrator Richtlinien ändern darf.	Ja, Nein Standard: Ja
Gruppen kopieren/ einfügen	Geben Sie an, ob der Gruppenadministrator Untergruppen kopieren und einfügen darf.	Ja, Nein Standard: Ja
Geräte entfernen	Geben Sie an, ob der Gruppenadministrator Geräte entfernen darf.	Ja, Nein Standard: Ja
Gruppen entfernen	Geben Sie an, ob der Gruppenadministrator Untergruppen entfernen darf.	Ja, Nein Standard: Ja
Benutzer entfernen	Geben Sie an, ob der Gruppenadministrator Benutzer entfernen darf.	Ja, Nein Standard: Ja
Benutzer von Unternehmen entfernen	Geben Sie an, ob der Gruppenadministrator Benutzer vom Unternehmen entfernen darf.	Ja, Nein Standard: Nein

Authentifizierungsrichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die Rechte und Berechtigungen von Unternehmens- und Gruppenauthentifizierern bestimmen.

TABELLE 9-5. Beschreibung der Administratorrichtlinien für PolicyServer

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Geräte hinzufügen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer Geräte hinzufügen dürfen.	Ja, Nein Standard: Nein
Benutzer hinzufügen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer neue Benutzer hinzufügen dürfen.	Ja, Nein Standard: Nein
Benutzer zu Unternehmen hinzufügen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer neue Benutzer zum Unternehmen hinzufügen dürfen.	Ja, Nein Standard: Nein
Gruppen hinzufügen/ ändern	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer Untergruppen hinzufügen/ändern dürfen.	Ja, Nein Standard: Nein
Gruppen kopieren/einfügen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer Untergruppen kopieren und einfügen dürfen.	Ja, Nein Standard: Nein
Geräte entfernen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer Geräte entfernen dürfen.	Ja, Nein Standard: Nein
Gruppen entfernen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer Untergruppen entfernen dürfen.	Ja, Nein Standard: Nein
Benutzer entfernen	Geben Sie an, ob Unternehmens- und Gruppenauthentifizierer Benutzer entfernen dürfen.	Ja, Nein Standard: Nein

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Benutzer von Unternehmen entfernen	Geben Sie an, ob Authentifizierer Benutzer vom Unternehmen entfernen dürfen.	Ja, Nein Standard: Nein

Richtlinien für Protokollwarnungen

In der folgenden Tabelle werden die Richtlinien in Bezug auf E-Mail-Nachrichten beschrieben, die bei wichtigen PolicyServer Protokollereignissen versendet werden.

Tabelle 9-6. Beschreibung der Richtlinie zu PolicyServer Protokollwarnungen

Name der Richtlinie	Beschreibung	Wertebereich und Standard
E-Mail-Absenderadresse	Geben Sie die E-Mail-Adresse an, die als Quell-E-Mail-Adresse für die Warnungsbenachrichtigungen verwendet wird.	1-255 Zeichen Standard: n. v.
SMTP-Servername	Geben Sie den SMTP-Server an, der für das Senden von E-Mail-Nachrichten mit Warnungen verantwortlich ist.	1-255 Zeichen Standard: n. v.

Richtlinien für das Herunterladen von Service Packs

In der folgenden Tabelle werden die Richtlinien beschrieben, die bestimmen, wann Agents Service Packs automatisch herunterladen.

TABELLE 9-7. Beschreibung der Richtlinien zum Herunterladen von PolicyServer Service-Packs

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Stunde, zu der das Herunterladen von Service Packs beginnt	Legen Sie die Zeit zum Herunterladen von Service Packs fest.	0-23 Standard: 0
Stunde, zu der das Herunterladen von Service Packs beendet wird	Legen Sie die Zeit fest, zu der das Herunterladen von Service Packs beendet wird.	0-23 Standard: 0

Richtlinien für Begrüßungsnachricht

In der folgenden Tabelle werden die Richtlinien beschrieben, die regeln, ob eine Begrüßungsnachricht an Benutzer gesendet wird, nachdem diese zu einer Gruppe hinzugefügt wurden.

TABELLE 9-8. Beschreibung der Richtlinien zur PolicyServer Begrüßungsnachricht

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Nachricht	Enthält die Datei mit der Begrüßungsnachricht.	1-1024 Zeichen Standard: n. v.
SMTP-Servername	Geben Sie den SMTP-Server an, der für das Senden von Begrüßungsnachrichten per E-Mail verantwortlich ist.	1-255 Zeichen Standard: n. v.
Quell-E-Mail	Geben Sie die E-Mail-Adresse an, die als Quell-E-Mail-Adresse für die Begrüßungsnachricht per E-Mail verwendet wird.	1-255 Zeichen Standard: n. v.
Betreff	Die Betreffzeile der Begrüßungsnachricht.	1-255 Zeichen Standard: n. v.

Richtlinien für Full Disk Encryption

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Richtlinien erläutert, die sich auf die folgenden Full Disk Encryption Agents auswirken.

- Full Disk Encryption
- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

Client-Richtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die sich auf den Zugriff auf die Full Disk Encryption Wiederherstellungskonsole und die Deinstallation des Agent auswirken.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

TABELLE 9-9. Beschreibung der Client-Richtlinien für Full Disk Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Wiederherstellung durch Benutzer zulassen	Geben Sie an, ob Benutzer auf dem Gerät auf Dienstprogramme für die Systemwiederherstellung zugreifen können.	Ja, Nein Standard: Nein
Deinstallation durch Benutzer zulassen	Geben Sie an, ob Full Disk Encryption vom Benutzer deinstalliert werden kann.	Ja, Nein Standard: Nein

Verschlüsselungsrichtlinien

In der folgenden Tabelle wird die Verschlüsselungsrichtlinie von Full Disk Encryption beschrieben. Eine Richtlinie zur Geräteverschlüsselung wirkt sich auf die Agents von Full Disk Encryption, der Encryption Management for Apple FileVault und der Encryption Management for Microsoft BitLocker aus.

TABELLE 9-10. Beschreibung der Verschlüsselungsrichtlinien für "Full Disk Encryption"

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Gerät verschlüsseln	Sie können angeben, ob das Gerät verschlüsselt werden soll.	Ja, Nein Standard: Ja

Anmelderichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die Anmeldung beim Full Disk Encryption Agent bestimmen.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

TABELLE 9-11. Beschreibung der Anmelderichtlinien für Full Disk Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Kontosperraktion	Legen Sie die Aktion fest, die durchgeführt werden soll, wenn das Gerät keine Kommunikation mit dem PolicyServer entsprechend der Festlegung in der Richtlinie "Zeitraum bis Kontosperrung" aufbaut. • Löschen: Der gesamte Inhalt auf dem Gerät wird gelöscht. • Remote-Authentifizierung: Erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt.	Löschen, Remote-Authentifizierung Standard: Remote-Authentifizierung
Zeitraum bis Kontosperrung	Geben Sie die Anzahl der Tage an, die für den Client ohne Kommunikation mit dem PolicyServer zulässig sind.	0-999 Standard: 360
Kennwort zur Auslöschung	Geben Sie eine Zeichenfolge an, bei deren Eingabe der gesamte Inhalt auf dem Gerät gelöscht wird.	1-255 Zeichen Standard: n. v.
Aktion zur Gerätesperrung	Geben Sie die Aktion an, die durchgeführt wird, wenn das Gerät gesperrt wird. • Zeitverzögerung: Der Zeitraum, der vergehen muss, bis der Benutzer sich erneut Anmelden kann. • Löschen: Der gesamte Inhalt auf dem Gerät wird gelöscht. • Remote-Authentifizierung: Erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt.	Zeitverzögerung, Löschen, Remote-Authentifizierung Standard: Zeitverzögerung

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Geben Sie die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche an, bevor die Zeitverzögerung zur Gerätesperre aktiviert wird.	0-100 Standard: 5
Falls gefunden	Geben Sie die anzuzeigenden Informationen an.	1-255 Zeichen Standard: n. v.
Rechtlicher Hinweis	Geben Sie an, ob ein rechtlicher Hinweis angezeigt werden soll.	Aktivieren/Deaktivieren Standard: Deaktiviert
Anzeigezeit für den rechtlichen Hinweis	Geben Sie an, wann dem Benutzer der rechtliche Hinweis angezeigt werden soll.	Installation, Start Standard: Start
Text des rechtlichen Hinweises	Geben Sie den Text des rechtlichen Hinweises an.	Datei einfügen Standard: n. v.
Zeitverzögerung bei Gerätesperre	Gerät für X Minuten sperren, wenn der Benutzer die zulässige Anzahl fehlgeschlagener Anmeldeversuche überschreitet.	1-999.999 Minuten Standard: 1
Preboot-Umgehung	Geben Sie an, ob Preboot umgangen werden soll.	Ja, Nein Standard: Nein
Support-Informationen	Zeigt Informationen zum Helpdesk bzw. den Administratorkontakt an.	Standard: n. v.
Token-Authentifizierung	Richtlinie hinsichtlich physischer Token, einschließlich Smartcards und USB-Token. Alle Unterrichtlinien sind nur sichtbar, wenn die Token-Authentifizierung aktiviert ist.	Aktivieren, Deaktivieren Standard: Deaktiviert

Name der Richtlinie	Beschreibung	Wertebereich und Standard
OCSP-Validierung	Das Verifizieren der Zertifikate über OCSP ermöglicht das Widerrufen ungültiger Zertifikate durch die Zertifizierungsstelle. **Hinweis** Alle Unterrichtlinien sind nur sichtbar, wenn die OCSP-Validierung aktiviert ist.	Aktivieren, Deaktivieren Standard: Deaktiviert
OCSP-CA-Zertifikate	Zertifikate der Zertifizierungsstelle. **Hinweis** Dabei handelt es sich um die Unterrichtlinie für die OCSP-Validierung.	0-1024 Zeichen Standard: n. v.
OCSP - Aktion bei Zertifikatsstatus 'Abgelaufen'	Definiert die Aktion, die bei Ablauf des OCSP-Zertifikatsstatus ausgeführt wird. **Hinweis** Dabei handelt es sich um die Unterrichtlinie für die OCSP-Validierung.	Zeitverzögerung, Löschen, Remote-Authentifizierung, Anmeldung verweigern, Zugriff zulassen Standard: Anmeldung verweigern
OCSP-Übergangsfrist	Eine Übergangsfrist in Tagen, in der die Authentifizierung erfolgen kann, selbst wenn der OCSP-Server das Zertifikat innerhalb dieser Frist nicht verifiziert hat. **Hinweis** Dabei handelt es sich um die Unterrichtlinie für die OCSP-Validierung.	0-365 Standard: 7

Name der Richtlinie	Beschreibung	Wertebereich und Standard
OCSP-Responder	Zertifikate der Zertifizierungsstelle. **Hinweis** Dabei handelt es sich um die Unterrichtlinie für die OCSP-Validierung.	Ja, Nein Standard: Ja
OCSP-Responder-Zertifikat	Zertifikat der Zertifizierungsstelle **Hinweis** Dabei handelt es sich um eine Unterrichtlinie für die OCSP-Responder.	0-1024 Zeichen Standard: n. v.
OCSP-Responder-URL	Zertifikate der Zertifizierungsstelle. **Hinweis** Dabei handelt es sich um eine Unterrichtlinie für die OCSP-Responder.	0-1024 Zeichen Standard: n. v.
OCSP - Aktion bei Zertifikatsstatus 'Widerrufen'	Definiert die Aktion, die bei Widerruf des OCSP-Zertifikatsstatus ausgeführt wird. **Hinweis** Dabei handelt es sich um eine Unterrichtlinie für die OCSP-Responder.	Zeitverzögerung, Löschen, Remote-Authentifizierung, Anmeldung verweigern, Zugriff zulassen Standard: Anmeldung verweigern

Name der Richtlinie	Beschreibung	Wertebereich und Standard
OCSP - Erfolg anzeigen	Ob der Erfolg der OCSP-Anwort angezeigt werden soll. **Hinweis** Dabei handelt es sich um eine Unterrichtlinie für die OCSP-Responder.	Ja, Nein Standard: Ja
OCSP - Aktion bei Zertifikatsstatus 'Unbekannt'	Geben Sie die Aktion an, die durchgeführt wird, wenn der OCSP-Zertifikatsstatus 'Unbekannt' lautet. Dabei handelt es sich um eine Unterrichtlinie für die OCSP-Responder.	Zeitverzögerung, Löschen, Remote-Authentifizierung, Anmeldung verweigern, Zugriff zulassen Standard: Anmeldung verweigern
Token-Durchleitung	Das Token wird während des Startvorgangs zur weiteren Verarbeitung an Desktop-GINA übergeben. Dabei handelt es sich um eine Unterrichtlinie für die OCSP-Responder.	Ja, Nein Standard: Nein

Kennwortrichtlinien

In der folgenden Tabelle werden die Kennwortrichtlinien von Full Disk Encryption beschrieben.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

TABELLE 9-12. Beschreibung der Kennwortrichtlinien für Full Disk Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Zulässige Authentifizierungsmethoden	Geben Sie die zulässigen Authentifizierungsmethoden an, die verwendet werden können.	Fest, ColorCode, PIN, Remote, RSA Standard: Fest

File Encryption Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Richtlinien erläutert, die sich auf File Encryption Agents auswirken.

Computerrichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die Installationsberechtigungen auf Geräten mit installierter File Encryption beschrieben.

TABELLE 9-13. Beschreibung der Computerrichtlinien für File Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Deinstallation durch Benutzer zulassen	Diese Richtlinien gibt an, ob ein anderer Benutzer als der Administrator die Endpunktanwendung deinstallieren kann.	Ja, Nein Standard: Ja

Verschlüsselungsrichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die bestimmen, wie die Verschlüsselung auf File Encryption Geräten gehandhabt wird.

TABELLE 9-14. Beschreibung der Verschlüsselungsrichtlinien für File Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Sicheres Löschen zulassen	Geben Sie an, ob der Benutzer Dateien löschen darf.	Ja, Nein Standard: Ja
Optisches Laufwerk deaktivieren	Deaktivieren Sie den Zugriff auf CD- bzw. DVD-Laufwerke.	Ja, Nein Standard: Nein

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Verwendeter Verschlüsselungsschlüssel	• Benutzerschlüssel: Wählen Sie einen für den Benutzer eindeutigen Schlüssel aus. • Gruppenschlüssel: Wählen Sie einen für die Gruppe eindeutigen Schlüssel aus, damit auch alle Benutzer in der Gruppe auf die Dateien zugreifen können. • Unternehmensschlüssel: Wählen Sie einen für das Unternehmen eindeutigen Schlüssel aus, damit auch alle Benutzer im Unternehmen auf die Dateien zugreifen können.	Benutzerschlüssel, Gruppenschlüssel, Unternehmensschlüssel Standard: Gruppenschlüssel
Zulässige Verschlüsselungsmethode	Wählen Sie die zulässigen Methoden zum Verschlüsseln von Dateien aus: • Benutzerschlüssel • Gruppenschlüssel • Benutzerdefiniertes Kennwort • Digitale Zertifikate	Eindeutiger Schlüssel des Benutzers, Eindeutiger Schlüssel der Gruppe, Mit statischem Kennwort verschlüsseln, Mit Zertifikat verschlüsseln Standard: Alle
Gerät vollständig verschlüsseln	Geben Sie an, ob alle Dateien/Ordner auf den Wechselmedien verschlüsselt werden sollen.	Ja, Nein Standard: Nein

Name der Richtlinie	Beschreibung	Wertebereich und Standard
USB-Geräte zulassen	Geben Sie die zulässigen USB-Geräte an.	Alle, KeyArmor Standard: Beliebig
USB-Laufwerk deaktivieren	Deaktivieren Sie das USB-Laufwerk, wenn es nicht angemeldet ist, deaktivieren Sie es immer oder niemals.	Immer, Abgemeldet, Niemals Standard: Abgemeldet
Zu verschlüsselnde Ordner auf Wechselmedien	Der Laufwerksbuchstabe ist vorgegeben und der Richtlinienwert entspricht einem gültigen Wechselmedium. Nicht vorhandene Ordner werden erstellt. Wenn kein Laufwerksbuchstabe angegeben wird, verwenden alle bei der Anmeldung am Gerät angeschlossenen Wechselmedien die Richtlinienwerte.	1-255 Zeichen Standard: n. v.
Ordner zum Verschlüsseln angeben	Listen Sie die Ordner auf, die auf der Festplatte verschlüsselt werden sollen. Nicht vorhandene Ordner werden erstellt. Außerdem muss auf dem Festplattenlaufwerk ein gültiger Laufwerksbuchstabe bereitgestellt werden. Ein gültiger Richtlinienwert lautet: C:\EncryptedFolder.	1-255 Zeichen Standard: `%DESKTOP%\Encrypted Files`

Anmelderichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die Anmeldung beim File Encryption Agent bestimmen.

TABELLE 9-15. Beschreibung der Anmelderichtlinien für File Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Zulässige Authentifizierungsmethoden	Geben Sie die zulässigen Authentifizierungstypen an, die verwendet werden können.	Fest, ColorCode, PIN, Smartcard, RSA Standard: Fest
Aktion zur Gerätesperrung	Die durchzuführende Aktion, wenn das Gerät gesperrt ist.	Zeitverzögerung, Remote-Authentifizierung Standard: Zeitverzögerung
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Anzahl der fehlgeschlagenen Anmeldeversuche, bevor die Zeitverzögerung bei Gerätesperre aktiviert wird. 0 ermöglicht eine unbegrenzte Anzahl an Versuchen.	0-100 Standard: 5
Anzeigezeit für den rechtlichen Hinweis **Hinweis** Dabei handelt es sich um die Unterrichtlinie für den rechtlichen Hinweis.	Geben Sie an, wann dem Benutzer der rechtliche Hinweis angezeigt wird. **Hinweis** Der rechtliche Hinweis wird nicht für File Encryption 3.1.3 oder ältere Agents angezeigt.	Installation, Start Standard: Start
Text des rechtlichen Hinweises **Hinweis** Dabei handelt es sich um die Unterrichtlinie für den rechtlichen Hinweis.	Geben Sie den Text des rechtlichen Hinweises an. **Hinweis** Der rechtliche Hinweis wird nicht für File Encryption 3.1.3 oder ältere Agents angezeigt.	Datei einfügen Standard: n. v.

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Zeitverzögerung bei Gerätesperre	Gerät für X Minuten sperren, wenn der Benutzer die zulässige Anzahl fehlgeschlagener Anmeldeversuche überschreitet.	0-999,999 Standard: 1

Kennwortrichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die File Encryption Kennwörter betreffen.

Tabelle 9-16. Beschreibung der Kennwortrichtlinien für File Encryption

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Kommunikation mit Server erzwingen	Erzwingt, dass der File Encryption Agent mit dem Server nach X Tagen kommuniziert. Bei einer Eingabe von 0 ist der File Encryption Agent eigenständig.	0-999 Standard: 360
Physischer Token erforderlich	Erfordert, dass ein physischer Token (Smartcard) zur Anmeldung bei Endpoint Encryption Geräten verwendet wird.	Ja, Nein Standard: Nein

Allgemeine Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Unternehmensrichtlinien erläutert, die sich auf alle Endpoint Encryption Agents auswirken.

Agent-Richtlinie

In der folgenden Tabelle wird die Richtlinie "Synchronisierungsintervall" erklärt.

TABELLE 9-17. Beschreibung der allgemeinen Agent-Richtlinien für Endpoint Encryption

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Synchronisierungsintervall	Geben Sie an, wie oft (in Minuten) die Anwendung mit PolicyServer kommuniziert, um aktualisierte Informationen zu erhalten.	1-1440 Standard: 30

Authentifizierungsrichtlinien

In der folgenden Tabelle werden die Richtlinien beschrieben, die die Authentifizierung von lokalen und Domänenbenutzerkonten bestimmen.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

TABELLE 9-18. Beschreibung der allgemeinen Authentifizierungsrichtlinien für Endpoint Encryption

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
n. v.	Offline-Änderung von Kennwörtern zulassen	Geben Sie an, ob Benutzer ihr Kennwort ändern können, wenn sie nicht mit PolicyServer verbunden sind.	Ja, Nein Standard: Nein

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung	Admin-Kennwort	Geben Sie Richtlinien zur ausschließlichen lokalen Authentifizierung am Gerät an.	n. v.
Lokale Anmeldung > **Admin-Kennwort**	Zulässige Zeichentypen	Geben Sie an, ob Kennwörter alphanumerische Zeichen, Ziffern, Sonderzeichen oder eine Kombination dieser enthalten dürfen.	Buchstaben, Zahlen und Sonderzeichen Standard: Alle
Lokale Anmeldung > **Admin-Kennwort**	Kann Benutzernamen enthalten	Geben Sie an, ob der Benutzername im Kennwort enthalten sein darf.	Ja, Nein Standard: Ja
Lokale Anmeldung > **Admin-Kennwort**	Zulässige aufeinanderfolgende Zeichen	Geben Sie die Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort an.	0-255 Standard: 3
Lokale Anmeldung > **Admin-Kennwort**	Mindestlänge	Geben Sie die zulässige Mindestlänge für Kennwörter an.	0-255 Standard: 6
Lokale Anmeldung > **Admin-Kennwort**	Aufbewahrung des Kennwortverlaufs	Geben Sie die Anzahl der vorherigen Kennwörter an, die der Benutzer nicht verwenden darf.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Zeichen	Geben Sie die Anzahl an Buchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Kleinbuchstaben	Geben Sie die Anzahl an Kleinbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Ziffern	Geben Sie die Anzahl an numerischen Zeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Sonderzeichen	Geben Sie die Anzahl an Sonderzeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Großbuchstaben	Geben Sie die Anzahl an Großbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung	Selbsthilfe	Geben Sie die Richtlinien für die Selbsthilfe an.	n. v.
Lokale Anmeldung > **Selbsthilfe**	Anzahl der Fragen	Geben Sie die Anzahl der Fragen an, die korrekt beantwortet werden müssen, um den Benutzer zu authentifizieren.	1-6 Standard: 1
Lokale Anmeldung > **Selbsthilfe**	Persönliche Herausforderung	Geben Sie die persönliche(n) Herausforderungsfrage(n) für die Selbsthilfe an.	1-1024 Standard: n. v.
Lokale Anmeldung	Benutzerkennwort	Geben Sie die Richtlinien an, die für Benutzerkennwörter verwendet werden.	n. v.
Lokale Anmeldung > **Benutzerkennwort**	Zulässige Zeichentypen	Geben Sie an, ob Kennwörter alphanumerische Zeichen, Ziffern, Sonderzeichen oder eine Kombination dieser enthalten dürfen.	Buchstaben, Zahlen und Sonderzeichen Standard: Alle

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung > **Benutzerkennwort**	Kann Benutzernamen enthalten	Geben Sie an, ob der Benutzername im Kennwort enthalten sein darf.	Ja, Nein Standard: Ja
Lokale Anmeldung > **Benutzerkennwort**	Kennwort ändern alle	Geben Sie (in Tagen) an, wann ein Benutzer sein Kennwort ändern muss.	1-1000000 Standard: 60
Lokale Anmeldung > **Benutzerkennwort**	Zulässige aufeinanderfolgende Zeichen	Geben Sie die Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort an.	0-255 Standard: 3
Lokale Anmeldung > **Benutzerkennwort**	Mindestlänge	Geben Sie die zulässige Mindestlänge für Kennwörter an.	0-255 Standard: 6
Lokale Anmeldung > **Benutzerkennwort**	Aufbewahrung des Kennwortverlaufs	Geben Sie die Anzahl der vorherigen Kennwörter an, die der Benutzer nicht verwenden darf.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Zeichen	Geben Sie die Anzahl an Buchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Kleinbuchstaben	Geben Sie die Anzahl an Kleinbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Ziffern	Geben Sie die Anzahl an numerischen Zeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Sonderzeichen	Geben Sie die Anzahl an Sonderzeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Großbuchstaben	Geben Sie die Anzahl an Großbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Bei Benutzernamen Schreibung beachten	Geben Sie an, ob im Benutzernamen die Groß- und Kleinschreibung beachtet werden soll.	Ja, Nein Standard: Nein
Netzwerkanmeldung	Eindeutiger Name	Optional: Geben Sie den eindeutigen Namen des Authentifizierungsservers an. Wird kein eindeutiger Name angegeben, wird die Standardnamenskonvention des LDAP-Servers verwendet.	1-255 Standard: n. v.
Netzwerkanmeldung	Domänenauthentifizierung	Gibt an, ob die Windows Anmeldedaten zum Authentifizieren verwendet werden sollen.	Ja, Nein Standard: Nein
Netzwerkanmeldung	Domänenname	NetBIOS-Name der Domäne für Single Sign On. Standard ist der vom PolicyServer verwendete NetBIOS-Wert.	1-255 Standard: n. v.
Netzwerkanmeldung	Host-Name	Geben Sie den Host-Namen an. Der Host-Name kann ein Domänenname sein.	1-255 Standard: n. v.

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Netzwerkanmeldung	Portnummer	Optional: 0 = Standard verwenden. Gibt den für die Verbindung zu verwendenden Port an. Wenn keine Portnummer angegeben wird, verwendet der LDAP-Anbieter die standardmäßige Portnummer.	0-65535 Standard: 0
Netzwerkanmeldung	Servertyp	Servertyp, der zum Authentifizieren der Anforderungen des Client-Benutzers verwendet wird.	LDAP, LDAProxy Standard: LDAP
Authentifizierung	Benutzer zwischen Anmeldungen speichern	Zuletzt verwendeten Benutzernamen speichern und auf dem Authentifizierungsbildschirm anzeigen.	Ja, Nein Standard: Ja

Kapitel 10

Gruppen in PolicyServer MMC

Endpoint Encryption verwendet sowohl die rollenbasierte als auch die identitätsbasierte Authentifzierung zum Sichern von Daten. Durch die ordnungsgemäße Konfiguration von Endpoint Encryption Gruppen wird sichergestellt, dass Daten für nicht autorisierte Benutzer verschlüsselt bleiben und das Risiko von Datenverlusten aufgrund versehentlicher Offenlegung oder beabsichtigter Sabotage vermieden werden kann.

Es werden folgende Themen behandelt:

- *Info über Gruppen auf Seite 10-2*
- *Gruppenverwaltung auf Seite 10-3*
- *Offline-Gruppen auf Seite 10-15*

Info über Gruppen

Gruppen werden in PolicyServer MMC verwaltet. In der folgenden Tabelle werden die verfügbaren Gruppentypen beschrieben.

TABELLE 10-1. PolicyServer Gruppentypen

GRUPPE	BESCHREIBUNG
Top-Gruppe	Die höchste Stufe der Gruppen im Unternehmen. Jede Top-Gruppe hat einen eindeutigen Knoten unterhalb des Unternehmens.
Untergruppe	Innerhalb einer Top-Gruppe erstellte Gruppen. Eine Untergruppe erbt die Richtlinien ihrer übergeordneten Gruppe. • Richtlinienvererbung findet nur statt, wenn eine Untergruppe erstellt wird. • Richtlinienänderungen an der Gruppe der obersten Ebene werden nicht bis in vorhandene Untergruppen weitergegeben. • Untergruppen-Richtlinien können nicht weniger strenge Einstellungen wie ihre übergeordneten Gruppen aufweisen.

Hinweis

Obwohl Untergruppen alle vorhandenen Richtlinien der übergeordneten Gruppe übernehmen, müssen Sie der Untergruppe Benutzer und Geräte gesondert hinzufügen.

Beim Hinzufügen von Endpoint Encryption Benutzer zu einer Untergruppe werden die Benutzer nicht automatisch zur Top-Gruppe hinzugefügt. Sie können jedoch Benutzer sowohl zur Top-Gruppe als auch zur Untergruppe hinzufügen.

Gruppenverwaltung

In diesem Abschnitt wird erklärt, wie Sie mit PolicyServer MMC neue Gruppen hinzufügen, Endpoint Encryption Benutzer und Geräte hinzufügen oder entfernen und Gruppen ändern.

Top-Gruppe hinzufügen

Gruppen vereinfachen die Verwaltung von Endpoint Encryption Agents, Benutzern, Richtlinien, Untergruppen und Geräten. Die Top-Gruppe ist die Gruppe auf der höchsten Stufe.

Hinweis

Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer Gruppen hinzuzufügen. Um einen Gruppenadministrator zu erstellen, fügen Sie einen Benutzer hinzu, und ändern Sie seine Kontoberechtigungen innerhalb der Gruppe. Weitere Informationen finden Sie unter *Benutzer ändern auf Seite 11-9*.

Prozedur

1. Klicken Sie mit der rechten Maustaste im linken Fenster auf das Unternehmen, und klicken Sie anschließend auf **Top-Gruppe hinzufügen**.

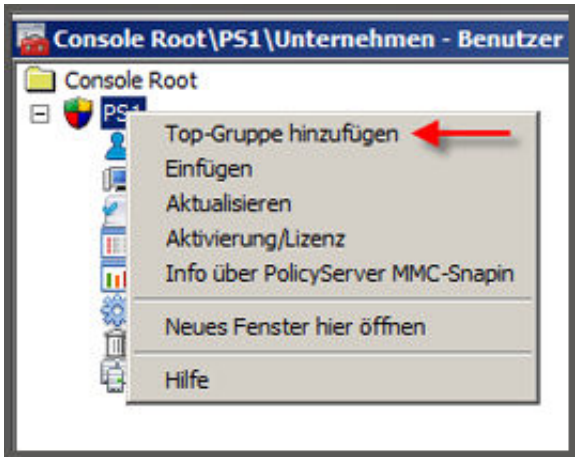


ABBILDUNG 10-1. Fenster "Top-Gruppe hinzufügen"

Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Geben Sie den Namen und eine Beschreibung der Gruppe an.

3. Wenn Endpoint Encryption Geräte verwendet werden, die Unicode nicht unterstützen, wählen Sie **Altgeräte unterstützen**.

Hinweis

Einige Altgeräte sind möglicherweise nicht in der Lage, unter Verwendung von Unicode mit PolicyServer zu kommunizieren. Weisen Sie Unicode-Geräte und ältere Endpoint Encryption Geräte verschiedenen Gruppen zu.

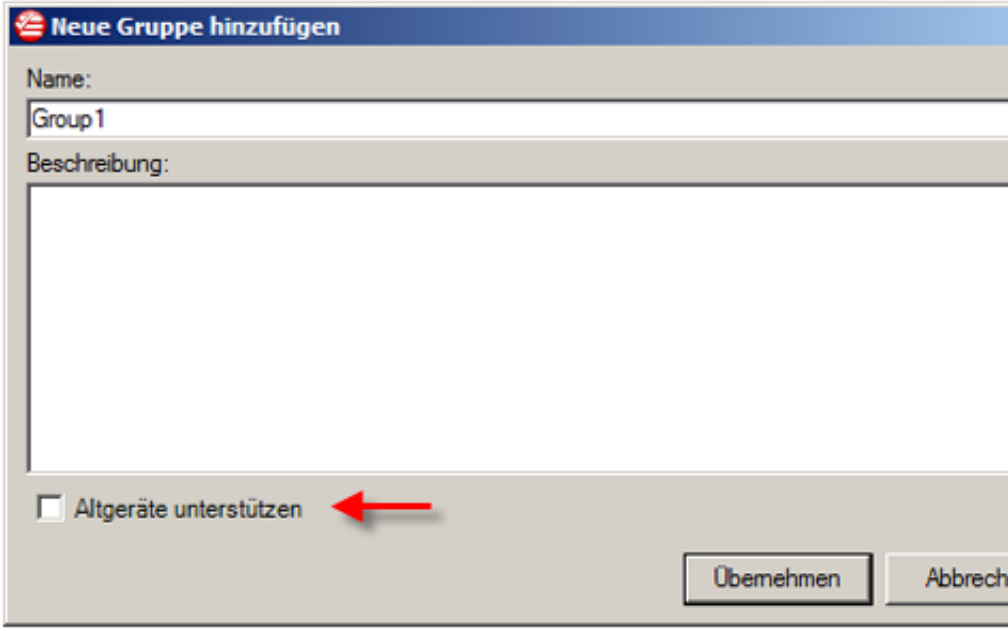


ABBILDUNG 10-2. Fenster "Neue Gruppe hinzufügen"

4. Klicken Sie auf **Übernehmen**.
5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

   Die neue Gruppe wird zur Baumstruktur im linken Fensterbereich hinzugefügt.

Untergruppe hinzufügen

Obwohl Untergruppen alle vorhandenen Richtlinien der übergeordneten Gruppe übernehmen, müssen Sie der Untergruppe Benutzer und Geräte gesondert hinzufügen.

Prozedur

1. Klicken Sie mit der rechten Maustaste in die linke Fensterstruktur und klicken Sie dann auf **Hinzufügen**.

Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Folgen Sie den Schritten in *Top-Gruppe hinzufügen auf Seite 8-7*.

   Die neue Gruppe wird der Baumstruktur innerhalb der Top-Gruppe hinzugefügt.

Gruppe ändern

Prozedur

1. Klicken Sie mit der rechten Maustaste in der linken Fensterstruktur auf eine Gruppe, und klicken Sie dann auf **Ändern**.

   Das Fenster **Gruppe ändern** wird angezeigt.

2. Geben Sie die Änderungen an.

3. Klicken Sie auf **Übernehmen**.

Gruppe entfernen

Verwenden Sie die Baumstruktur, um eine Gruppe zu entfernen. Wenn Sie eine Top-Gruppe entfernen, werden auch alle Untergruppen entfernt.

Prozedur

1. Klicken Sie mit der rechten Maustaste in der linken Fensterstruktur auf eine Gruppe, und klicken Sie dann auf **Entfernen**.

   Eine Warnmeldung wird angezeigt.

2. Klicken Sie auf **Ja**, um die Gruppe zu entfernen.

   Die ausgewählte Gruppe wird nicht mehr in der Baumstruktur angezeigt.

Neuen Benutzer zu einer Gruppe hinzufügen

Hinweis

Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.

Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.
2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Neuen Benutzer hinzufügen**.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

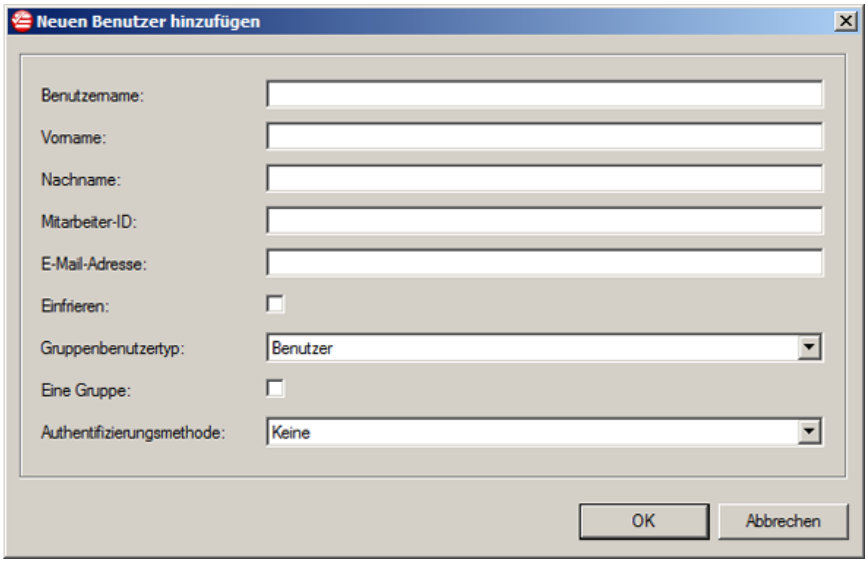


ABBILDUNG 10-3. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die folgenden Optionen an:

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen für das neue Benutzerkonto an (erforderlich).
Vorname	Geben Sie den Vornamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Nachname	Geben Sie den Nachnamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers für das neue Benutzerkonto an (optional).
Einfrieren	Wählen Sie, ob das neue Benutzerkonto vorübergehend deaktiviert werden soll (optional). Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräten anmelden.
Gruppenbenutzertyp	Wählen Sie die Berechtigungen für das neue Konto.

Option	Bezeichnung
	Hinweis Informationen über Kontorollen finden Sie unter *Endpoint Encryption Benutzerrollen auf Seite 2-6*. Zu den Optionen gehören: • Benutzer • Authentifizierer • Administrator **Hinweis** Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer zu Gruppen hinzuzufügen.
Eine Gruppe	Wählen Sie, ob das neue Benutzerkonto ein Mitglied von mehreren Gruppenrichtlinien sein darf.
Authentifizierungsmethode	Wählen Sie die Methode aus, mit der sich das neue Benutzerkonto an den Endpoint Encryption Geräten anmelden wird. **Hinweis** Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**. Informationen über Kontorollen finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*.

4. Klicken Sie auf **OK**.

Der neue Benutzer wird der ausgewählten Gruppe und zum Unternehmen hinzugefügt. Der Benutzer kann sich nun an den Endpoint Encryption Geräten anmelden.

Vorhandenen Benutzer zu einer Gruppe hinzufügen

Ein Benutzer kann in mehreren Gruppen Mitglied sein.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster, und klicken Sie auf **Benutzer**.
2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Vorhandenen Benutzer hinzufügen**.

   Das Fenster **Benutzer zu Gruppe hinzufügen** wird angezeigt.

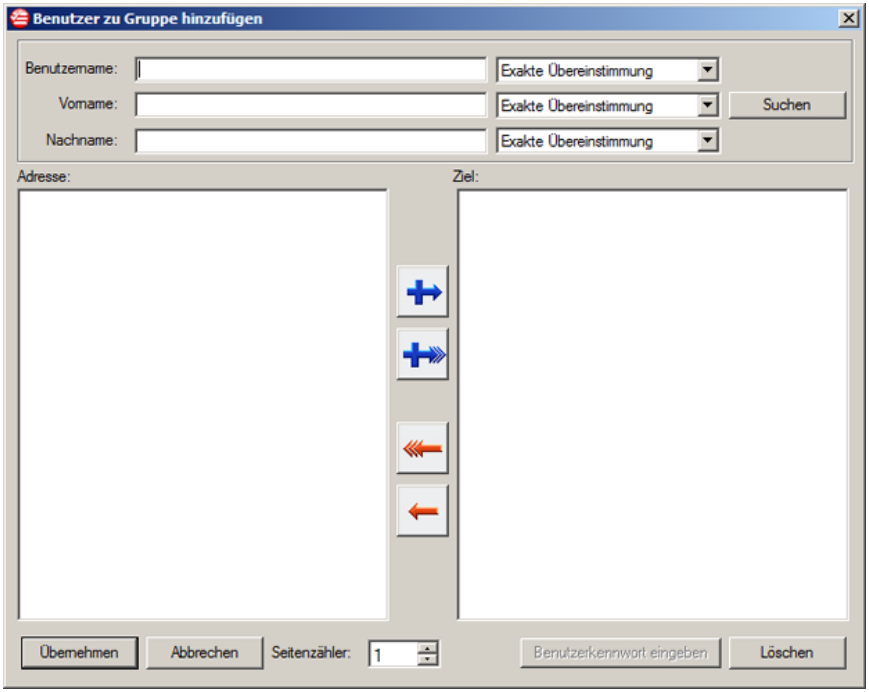


ABBILDUNG 10-4. Fenster "Benutzer zu Gruppe hinzufügen"

3. Geben Sie die Benutzerdetails ein und klicken Sie dann auf **Suchen**.

Im Feld **Quelle** werden die Konten angezeigt, die den Suchkriterien entsprechen.

4. Wählen Sie Benutzer aus der Liste im Feld **Quelle** aus, und klicken Sie auf den blauen Pfeil, um sie hinzufügen.

   Weitere Informationen zu Suchsymbolen finden Sie unter *Symbole für Suchergebnisse hinzufügen/entfernen auf Seite 11-15*.

   Der ausgewählte Benutzer wird in die Liste **Ziel** verschoben.

5. So ändern Sie ein Benutzerkennwort:

   a. Markieren Sie den Benutzer in der Liste **Ziel**.

   b. Klicken Sie im unteren Fensterbereich auf **Benutzerkennwort eingeben**.

   c. Geben Sie im anschließend angezeigten Fenster die Authentifizierungsmethode für den Benutzer an.

   d. Klicken Sie auf **Übernehmen**, um das Fenster **Kennwort ändern** zu schließen.

6. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

   Der Benutzer wird zur Gruppe hinzugefügt. Wenn es sich um die einzige Gruppenzuweisung handelt, kann sich der Benutzer nun bei den Endpoint Encryption Geräten anmelden.

Benutzer aus einer Gruppe entfernen

Warnung!

Bevor Sie einen Gruppenadministrator oder ein Gruppenauthentifiziererkonto entfernen, weisen Sie diese Rolle einem anderen Benutzerkonto zu. Andernfalls können nur der Unternehmensadministrator oder der Unternehmensauthentifizierer Änderungen an der Gruppe vornehmen.

Wenn Sie einen Benutzer aus einer Gruppe entfernen, kann der Benutzer nicht mehr auf Endpoint Encryption Geräte zugreifen, die dieser Gruppe zugeordnet sind. Bevor Sie Endpoint Encryption Benutzer entfernen, sollten Sie sich vergewissern, dass die Benutzer ihre Daten gesichert und entschlüsselt haben.

Prozedur

1. Erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Um den Benutzer ebenfalls vom Unternehmen zu entfernen, wählen Sie **Von Unternehmen entfernen**.

   Hinweis

   Beim Entfernen eines Benutzers vom Unternehmen wird der Benutzer ebenfalls aus allen Gruppen und Untergruppen entfernt.
4. Klicken Sie auf **Ja**.

   Der Benutzer wird entfernt.

Alle Benutzer aus einer Gruppe entfernen

Warnung!

Bevor Sie einen Gruppenadministrator oder ein Gruppenauthentifiziererkonto entfernen, weisen Sie diese Rolle einem anderen Benutzer zu. Andernfalls können nur der Unternehmensadministrator und der Unternehmensauthentifizierer Änderungen auf Gruppenebene vornehmen.

Prozedur

1. Erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Alle Benutzer entfernen** aus.

   Eine Warnmeldung wird angezeigt.

3. Um alle Benutzer ebenfalls vom Unternehmen zu entfernen, wählen Sie **Von Unternehmen entfernen**.

Hinweis

Beim Entfernen eines Benutzers vom Unternehmen wird der Benutzer ebenfalls aus allen Gruppen und Untergruppen entfernt.

4. Klicken Sie auf **Ja**.

Gerät zu einer Gruppe hinzufügen

Hinweis

Jedes Endpoint Encryption Gerät kann nur einer einzigen Gruppe angehören.

Prozedur

1. Erweitern Sie im linken Fenster die gewünschte Richtliniengruppe und klicken Sie auf **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät hinzufügen** aus.

Das Fenster **Geräte zu Gruppe hinzufügen** wird angezeigt.

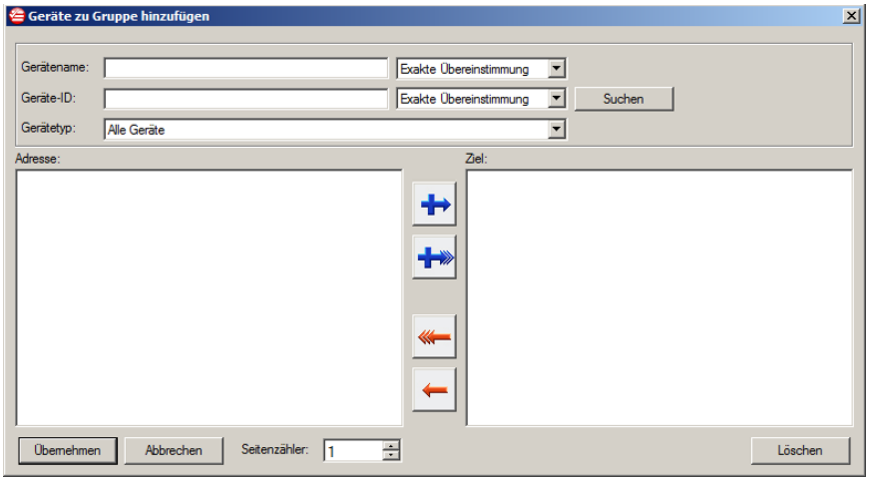


ABBILDUNG 10-5. Fenster Geräte zu Gruppe hinzufügen

3. Geben Sie die Gerätedetails ein, und klicken Sie dann auf **Suchen**.

   Wird eine Übereinstimmung gefunden, werden im Feld **Quelle** die Endpoint Encryption Geräte angezeigt.

4. Wählen Sie die entsprechenden Endpoint Encryption Geräte aus dem Feld **Quelle**, und klicken Sie anschließend auf den **blauen Pfeil**, um sie hinzuzufügen.

   Weitere Informationen zu Suchsymbolen finden Sie unter *Symbole für Suchergebnisse hinzufügen/entfernen auf Seite 11-15*.

5. Klicken Sie auf **Übernehmen**, um das Endpoint Encryption Gerät der ausgewählte Gruppe hinzuzufügen.

   Das Endpoint Encryption Gerät wird der Gruppe hinzugefügt.

Gerät aus einer Gruppe entfernen

Beim Löschen eines Geräts aus einer Gruppe wird das Gerät nur aus der ausgewählten Gruppe entfernt.

Warnung!

Um ein Gerät aus allen Gruppen zu entfernen, entfernen Sie es aus dem Unternehmen. Stellen Sie vor dem Löschen eines Geräts aus dem Unternehmen sicher, dass das Gerät entschlüsselt wurde und alle Endpoint Encryption Agents deinstalliert wurden. Falls Sie dies nicht tun, könnte dies zu irreversiblen Datenverlusten führen.

Prozedur

1. Erweitern Sie die Gruppe, und öffnen Sie dann **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Klicken Sie auf **Ja**.

   Das Gerät wird entfernt.

Offline-Gruppen

Bei einer Offline-Gruppe handelt es sich um eine Gruppe von Endpunkten, die keine Verbindung zum PolicyServer hatten, als der File Encryption Agent installiert wurde. Exportieren Sie die Richtlinien, Benutzer und Geräte für diese Gruppe in eine Datei, und installieren Sie sie auf jedem Endpunkt. Wenn an der Gruppe Änderungen erforderlich sind, exportieren Sie eine neue Datei, und wiederholen Sie den Import.

Richtlinien werden automatisch aktualisiert, wenn der Agent eine Verbindung zu PolicyServer herstellt.

Offline-Gruppe erstellen

Über Offline-Gruppen können Agents, die nicht mit PolicyServer kommunizieren können oder müssen, aktualisierte Richtlinien erhalten. Die Installationsdateien von Endpoint Encryption Agent müssen auf dem Server verfügbar sein, auf dem PolicyServer installiert ist.

Hinweis

Exportierte Gruppen müssen mindestens einen Benutzer enthalten. Der Gruppenname muss ebenfalls nur alphanumerisch sein.

Prozedur

1. Klicken Sie im linken Fenster mit der rechten Maustaste auf die Gruppe und wählen Sie **Exportieren** aus.

   Der **PolicyServer Assistent zum Exportieren von Gruppen** wird angezeigt.

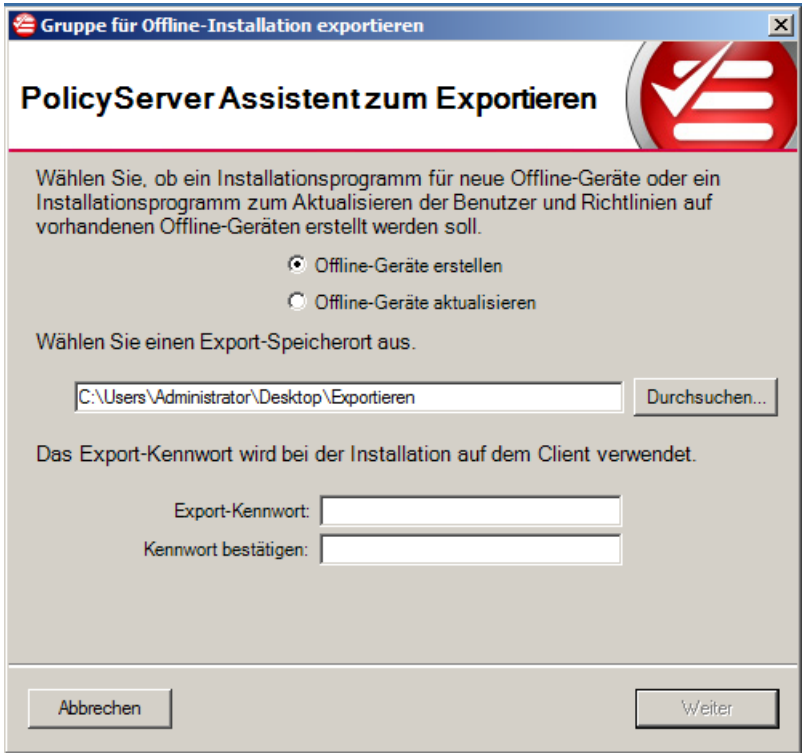

Gruppe für Offline-Installation exportieren
PolicyServer Assistent zum Exportieren
Wählen Sie, ob ein Installationsprogramm für neue Offline-Geräte oder ein Installationsprogramm zum Aktualisieren der Benutzer und Richtlinien auf vorhandenen Offline-Geräten erstellt werden soll.
Offline-Geräte erstellen
Offline-Geräte aktualisieren
Wählen Sie einen Export-Speicherort aus.
C:\Users\Administrator\Desktop\Exportieren
Durchsuchen...
Das Export-Kennwort wird bei der Installation auf dem Client verwendet.
Export-Kennwort:
Kennwort bestätigen:
Abbrechen
Weiter

ABBILDUNG 10-6. PolicyServer Assistent zum Exportieren von Gruppen

2. Wählen Sie **Offline-Geräte erstellen** aus.

3. Geben Sie den Speicherort für den Export an.

4. Geben Sie das Kennwort für den Export an, und bestätigen Sie es.

> **Hinweis**
>
> Das Exportkennwort wird zum Authentifizieren der ausführbaren Datei auf dem Agent verwendet.

5. Klicken Sie auf **Weiter**.

6. Klicken Sie auf **Hinzufügen**, um zu den Installationsprogrammen des Endpoint Encryption Clients zu navigieren und diese hochzuladen.

TABELLE 10-2. Dateiname der Endpoint Encryption Installationsdatei

INSTALLATIONSDATEI	ZWECK
`FileEncryptionIns.exe`	Installiert den File Encryption Agent.

> **Hinweis**
>
> Informationen zu älteren Versionen von Endpoint Encryption finden Sie in der begleitenden Dokumentation.

7. Klicken Sie auf **Weiter**.

8. Geben Sie je nach Lizenztyp die Anzahl der zu installierenden Geräte an. Die Anzahl der verfügbaren Lizenzen nimmt mit jedem Gerät ab.

9. Geben Sie optional einen **Präfix des Gerätenamens** an. PolicyServer verwendet die Gerätepräfixnummer, um eine eindeutige Geräte-ID und einen Verschlüsselungsschlüssel für jedes Gerät in dieser Gruppe zu erstellen.

10. Klicken Sie auf **Weiter**.

    Die Offline-Gruppe wird erstellt.

11. Klicken Sie auf **Fertig**, um eine Exportdatei am angegebenen Speicherort zu erstellen.

Eine erstellte ausführbare Datei namens „Export“ wird auf dem Desktop erstellt. Verwenden Sie diese, um Richtlinienänderungen an Offline-Gruppen zu verteilen.

Offline-Gruppe aktualisieren

Das folgende Verfahren beschreibt, wie Sie ein Update für eine Offline-Gruppe erstellen.

Prozedur

1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf die Gruppe, und wählen Sie anschließend **Exportieren** aus.

   Der **PolicyServer Assistent zum Exportieren von Gruppen** wird geöffnet.

2. Wählen Sie **Offline-Geräte aktualisieren**.

3. Geben Sie das Kennwort zum Exportieren ein.

   Hinweis

   Verwenden Sie das Exportkennwort zum Authentifizieren der ausführbaren Datei auf dem Endpoint Encryption Agent.

4. Klicken Sie auf **Durchsuchen**, um einen Speicherort für die Exportdatei auszuwählen.

5. Klicken Sie auf **Weiter**.

   Die Offline-Gruppe wird erstellt.

6. Klicken Sie auf **Fertig**.

   Die Exportdatei wird am angegebenen Speicherort erstellt.

7. Installieren Sie die Software auf dem Gerät mit einer generierten ausführbaren Datei oder einem Skript.

Hinweis

Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Kapitel 11

Benutzer in PolicyServer MMC

Endpoint Encryption verfügt über mehrere Typen von Kontorollen und Authentifizierungsmethoden, die eine umfassende, auf Identität basierende Authentifizierung und Verwaltung möglich machen. Mit Control Manager oder PolicyServer MMC können Sie Benutzerkonten hinzufügen oder importieren, die Authentifizierung steuern, mit Active Directory eine Synchronisierung durchführen und die Mitgliedschaft in Richtliniengruppen bei Bedarf verwalten.

Hinweis

Eine Beschreibung zu Benutzerrollen und Authentifizierung von Endpoint Encryption finden Sie unter *Endpoint Encryption Benutzer auf Seite 2-5*.

In diesem Kapitel werden die Kontorollen und Authentifizierungsmethoden, die Administrierung von PolicyServer MMC zur Verwaltung von Richtlinien, die sich auf Endpoint Encryption Benutzer auswirken, und die Steuerung des Informationszugriffs über den Richtlinienknoten **Benutzer** in PolicyServer MMC beschrieben. In diesem Kapitel wird ebenfalls erklärt, wie Sie gelöschte Endpoint Encryption Benutzer wiederherstellen.

Es werden folgende Themen behandelt:

- *Benutzer zu Endpoint Encryption hinzufügen auf Seite 6-4*
- *Benutzer suchen auf Seite 11-8*

- *Benutzer ändern auf Seite 11-9*
- *Neuen Benutzer zu einer Gruppe hinzufügen auf Seite 8-9*
- *Vorhandenen Benutzer zu einer Gruppe hinzufügen auf Seite 8-15*
- *Standardgruppe eines Benutzers ändern auf Seite 11-16*
- *Benutzer das Installieren in eine Gruppe erlauben auf Seite 11-17*
- *Benutzer aus einer Gruppe entfernen auf Seite 10-11*
- *Alle Benutzer aus einer Gruppe entfernen auf Seite 10-12*
- *Gelöschtes Benutzer wiederherstellen auf Seite 6-27*
- *Arbeiten mit Kennwörtern auf Seite 6-11*

Benutzer zu Endpoint Encryption hinzufügen

Endpoint Encryption verfügt über mehrere Möglichkeiten, um Benutzer zu Endpoint Encryption hinzuzufügen:

- Fügen Sie die Benutzer manuell nacheinander hinzu.
- Verwenden Sie die Massenimportfunktion für mehrere Benutzer mit einer CSV-Datei.
- Verwenden Sie den externen Verzeichnis-Browser mit Active Directory.

Neuen Unternehmensbenutzer hinzufügen

Das folgende Verfahren erklärt, wie Sie neue Endpoint Encryption Benutzer dem Unternehmen hinzufügen.

Hinweis

Wenn Sie einen neuen Endpoint Encryption Benutzer zum Unternehmen hinzufügen, wird der Benutzer keiner Gruppe zugewiesen.

Beim Hinzufügen eines Endpoint Encryption Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Gehen Sie wie folgt vor, um auf Benutzer im Unternehmen zuzugreifen:
   - Erweitern Sie das Unternehmen, und öffnen Sie anschließend **Unternehmen - Benutzer**.
   - Erweitern Sie das Unternehmen, erweitern Sie die Gruppe, und öffnen Sie anschließend **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf einen leeren Bereich im rechten Fensterbereich, und wählen Sie **Benutzer hinzufügen** aus.

Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

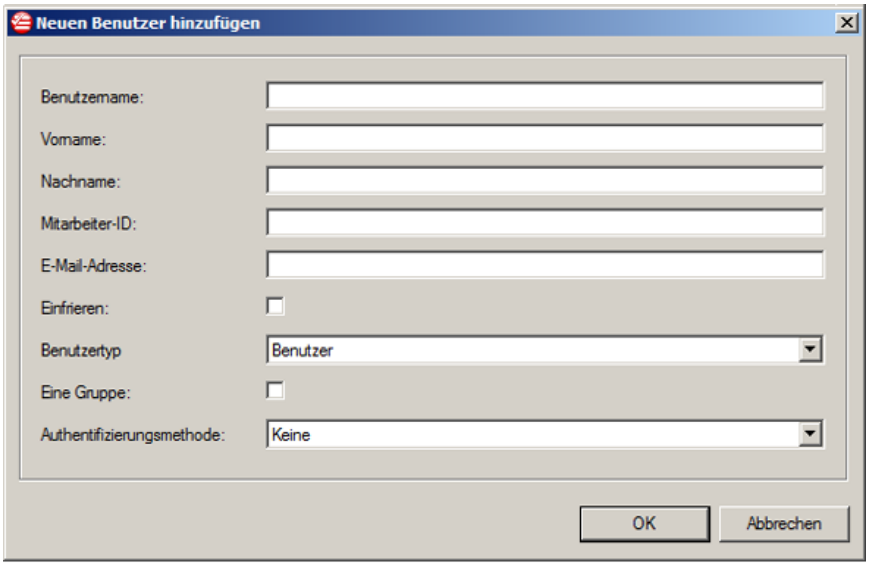


ABBILDUNG 11-1. FENSTER "NEUEN BENUTZER HINZUFÜGEN"

3. Geben Sie die folgenden Optionen an:

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen für das neue Benutzerkonto an (erforderlich).
Vorname	Geben Sie den Vornamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Nachname	Geben Sie den Nachnamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers für das neue Benutzerkonto an (optional).
Einfrieren	Wählen Sie, ob das neue Benutzerkonto vorübergehend deaktiviert werden soll (optional).

Option	Bezeichnung
	Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräten anmelden.
Gruppenbenutzertyp	Wählen Sie die Berechtigungen für das neue Konto. Informationen über Kontorollen finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*. Zu den Optionen gehören: • **Benutzer** • **Authentifizierer** • **Administrator** **Hinweis** Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer zu Gruppen hinzuzufügen.
Eine Gruppe	Wählen Sie, ob das neue Benutzerkonto ein Mitglied von mehreren Gruppenrichtlinien sein darf.
Authentifizierungsmethode	Wählen Sie die Methode aus, mit der sich das neue Benutzerkonto an den Endpoint Encryption Geräten anmelden wird. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*. **Hinweis** Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

4. Klicken Sie auf **OK**.

Der neue Endpoint Encryption Benutzer wird dem Unternehmen hinzugefügt. Der Benutzer kann sich zuerst bei Endpoint Encryption Geräten anmelden, nachdem das Benutzerkonto einer Gruppe hinzugefügt wurde.

Benutzer aus einer CSV-Datei importieren

Verwenden Sie eine kommagetrennte Datei (CSV), um mehrere Benutzer gleichzeitig zu importieren.

Format: Benutzername (erforderlich), Vorname, Nachname, Mitarbeiter-ID, E-Mail-Adresse

Hinweis

Verwenden Sie ein Komma für Felder ohne Daten.

Erstellen Sie unbedingt eine separate CSV-Datei für jede zu importierende Benutzergruppe. Alle Benutzer in der CSV-Datei werden derselben Gruppe hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster, und klicken Sie auf **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster, und wählen Sie dann **Massenimport zum Hinzufügen von Benutzern** aus.

   Das Fenster zum Öffnen der Datei wird angezeigt.
3. Navigieren Sie zur CSV-Datei und klicken Sie auf **Öffnen**.
4. Klicken Sie als Bestätigung auf **OK**.

   Die Benutzer in der CSV-Datei werden zur Gruppe und zum Unternehmen hinzugefügt.

Active Directory-Benutzer importieren

PolicyServer beinhaltet ein Benutzerverzeichnis getrennt von der Active Directory-Datenbank. Damit kann PolicyServer absolute Sicherheit für den Zugriff auf alle Endpoint Encryption Geräte, Benutzerrechte und Authentifizierungsmethoden gewährleisten.

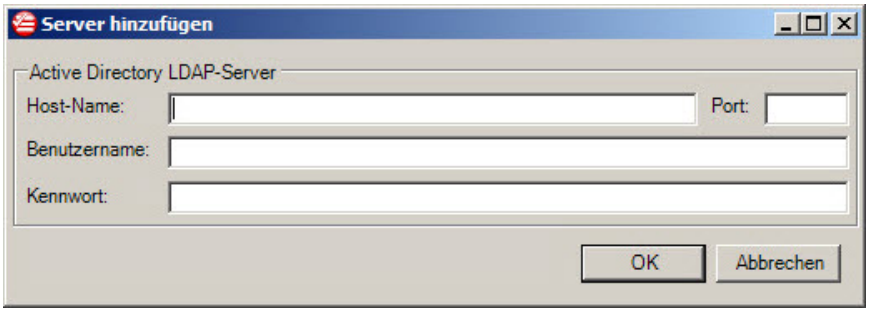
Informationen zur Konfiguration der Active Directory-Integration finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Öffnen Sie **Unternehmen - Benutzer**, klicken Sie mit der rechten Maustaste auf einen leeren Bereich im linken Fenster, und wählen Sie **Externer Verzeichnis-Browser** aus.

   Das Fenster **Active Directory-Benutzerimport** wird angezeigt.
3. Navigieren Sie zu **Bearbeiten** > **Mit Domäne verbinden**.

   Das Fenster **Server hinzufügen** wird angezeigt.



4. Geben Sie die folgenden Parameter für den Active Directory-LDAP-Server an:
   - **Host-Name**
   - **Port**
   - **Benutzername**
   - **Kennwort**
5. Klicken Sie auf **OK**.
6. Warten Sie darauf, dass die angegebe Active Directory-Domäne mit Daten gefüllt wird.

   Die Active Directory-Struktur für die angegebene Domäne wird im linken Fensterbereich angezeigt.

7. Wählen Sie in der Navigationsstruktur im linken Fensterbereich den Container, dem Benutzer hinzugefügt werden sollen.

   Die verfügbaren Benutzer werden im rechten Fensterbereich eingefügt.

8. Wählen Sie die betreffenden Benutzer, klicken Sie mit der rechten Maustaste auf die Auswahl, und wählen Sie anschließend:

   - **Zur Unternehmen hinzufügen**
   - **Zur Gruppe hinzufügen**

     a. Erweitern Sie den Knoten "Unternehmen".

     b. Wählen Sie die entsprechende Gruppe.

     c. Klicken Sie auf **OK**.

9. Klicken Sie auf **OK**, um die Benutzer zum angegebenen Speicherort hinzuzufügen.

   Eine Bestätigungsmeldung wird angezeigt.

10. Klicken Sie zur Bestätigung auf **OK**.

    Eine Importstatusmeldung wird angezeigt.

11. Klicken Sie auf **OK**, um den Schritt zu beenden, oder wiederholen Sie das Verfahren, um weitere Benutzer zum Importieren auszuwählen.

Benutzer suchen

Die Suche nach Benutzern auf Gruppenebene ist zwar schneller, bei dieser Methode muss jedoch das ganze Unternehmen durchsucht werden.

Prozedur

1. Klicken Sie im linken Fensterbereich auf **Unternehmen - Benutzer**, oder erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.

2. Klicken Sie in der oberen Ecke des rechten Fensters auf **Suchen**.

Das Fenster **Benutzersuchfilter** wird angezeigt.

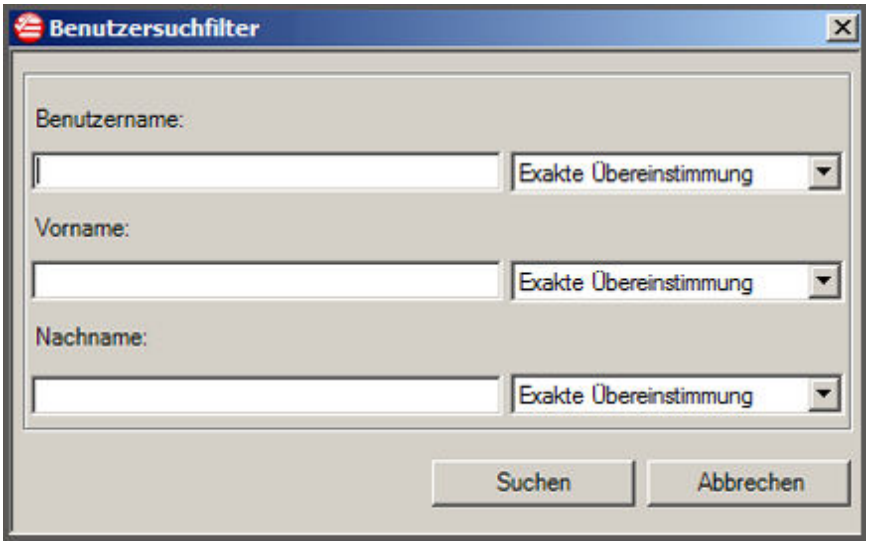


ABBILDUNG 11-2. Fenster "Benutzersuchfilter"

3. Geben Sie die Suchdetails ein und klicken Sie dann auf **Suchen**.

   Alle mit diesem Suchkriterium übereinstimmenden Konten werden angezeigt.

Hinweis

Verwenden Sie bei vielen Benutzern die Option **Seitenzähler**, um von einer Seite zur anderen zu wechseln, und klicken Sie auf **Löschen**, um alle Ergebnisse zu entfernen.

Benutzer ändern

Jeder Gruppenadministrator kann die Profilinformationen eines Benutzers ändern.

Hinweis

- Änderungen auf Unternehmensebene werden global auf den Benutzer angewendet, wohingegen sich Änderungen auf Gruppenebene nur auf eine bestimmte Gruppe beziehen.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den Benutzer, und wählen Sie anschließend **Benutzer ändern**.

   Das Fenster **Benutzer ändern** wird angezeigt.
3. Nehmen Sie die erforderlichen Änderungen vor. Wenn sich die Authentifizierungsmethoden-Änderungen in **Festes Kennwort** ändern, geben Sie das Standardbenutzerkennwort an.
4. Klicken Sie auf **OK**.
5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gruppenmitgliedschaft eines Benutzers anzeigen

Sie können eine Liste der Gruppen anzeigen, um die Gruppenmitgliedschaft des Endpoint Encryption Benutzers einzusehen. Bei Benutzern, die mehreren Gruppen angehören, können Sie auch die Priorität der zugewiesenen Gruppen ändern. Informationen zur Standardgruppe finden Sie unter *Standardgruppe eines Benutzers ändern auf Seite 11-16*.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer, und wählen Sie dann **Gruppen auflisten** aus.

Die Liste **Gruppenmitgliedschaft** wird angezeigt.

Neuen Benutzer zu einer Gruppe hinzufügen

Hinweis

Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.

Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.
2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Neuen Benutzer hinzufügen**.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

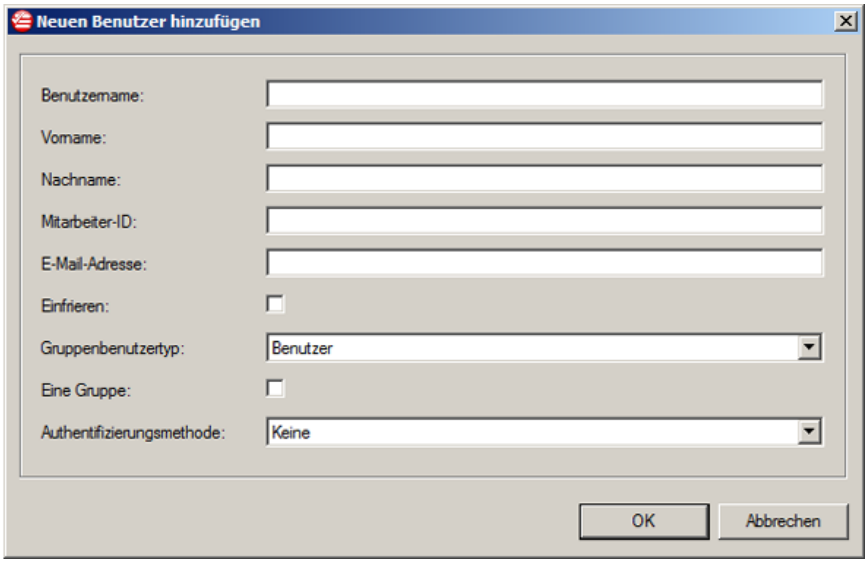


ABBILDUNG 11-3. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die folgenden Optionen an:

OPTION	BEZEICHNUNG
Benutzername	Geben Sie den Benutzernamen für das neue Benutzerkonto an (erforderlich).
Vorname	Geben Sie den Vornamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Nachname	Geben Sie den Nachnamen des Benutzers für das neue Benutzerkonto an (erforderlich).
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers für das neue Benutzerkonto an (optional).
Einfrieren	Wählen Sie, ob das neue Benutzerkonto vorübergehend deaktiviert werden soll (optional). Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräten anmelden.
Gruppenbenutzertyp	Wählen Sie die Berechtigungen für das neue Konto.

Option	Bezeichnung
	Hinweis Informationen über Kontorollen finden Sie unter *Endpoint Encryption Benutzerrollen auf Seite 2-6*. Zu den Optionen gehören: • Benutzer • Authentifizierer • Administrator **Hinweis** Es ist nicht möglich, die Konten Unternehmensadministrator oder Unternehmensauthentifizierer zu Gruppen hinzuzufügen.
Eine Gruppe	Wählen Sie, ob das neue Benutzerkonto ein Mitglied von mehreren Gruppenrichtlinien sein darf.
Authentifizierungsmethode	Wählen Sie die Methode aus, mit der sich das neue Benutzerkonto an den Endpoint Encryption Geräten anmelden wird. **Hinweis** Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**. Informationen über Kontorollen finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*.

4. Klicken Sie auf **OK**.

Der neue Benutzer wird der ausgewählten Gruppe und zum Unternehmen hinzugefügt. Der Benutzer kann sich nun an den Endpoint Encryption Geräten anmelden.

Vorhandenen Benutzer zu einer Gruppe hinzufügen

Ein Benutzer kann in mehreren Gruppen Mitglied sein.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster, und klicken Sie auf **Benutzer**.
2. Wechseln Sie in den rechten Fensterbereich, klicken Sie mit der rechten Maustaste auf einen freien Bereich, und wählen Sie anschließend **Vorhandenen Benutzer hinzufügen**.

   Das Fenster **Benutzer zu Gruppe hinzufügen** wird angezeigt.

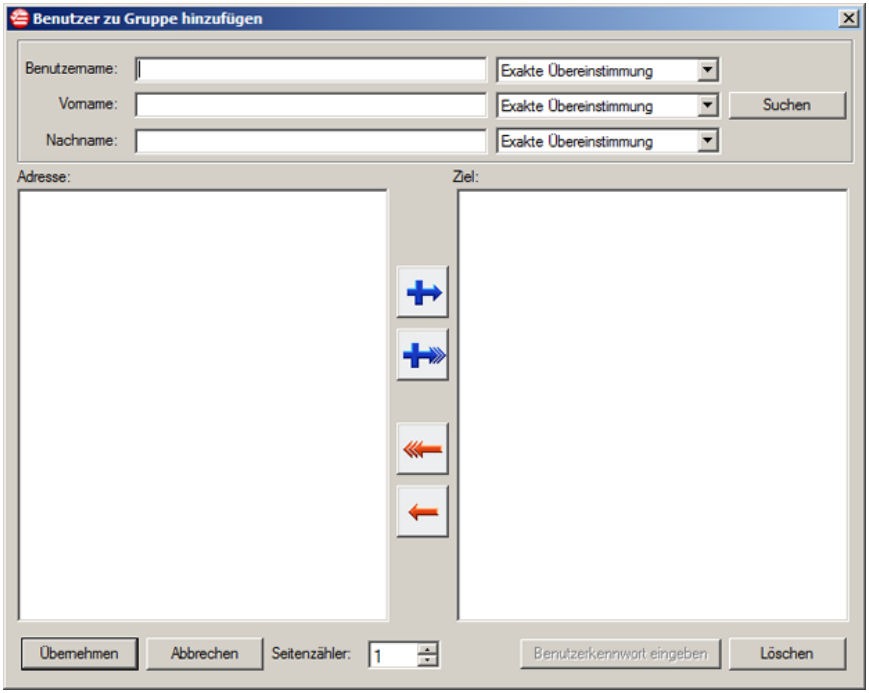


ABBILDUNG 11-4. Fenster "Benutzer zu Gruppe hinzufügen"

3. Geben Sie die Benutzerdetails ein und klicken Sie dann auf **Suchen**.

   Im Feld **Quelle** werden die Konten angezeigt, die den Suchkriterien entsprechen.

4. Wählen Sie Benutzer aus der Liste im Feld **Quelle** aus, und klicken Sie auf den blauen Pfeil, um sie hinzufügen.

   Weitere Informationen zu Suchsymbolen finden Sie unter *Symbole für Suchergebnisse hinzufügen/entfernen auf Seite 11-15*.

   Der ausgewählte Benutzer wird in die Liste **Ziel** verschoben.

5. So ändern Sie ein Benutzerkennwort:

   a. Markieren Sie den Benutzer in der Liste **Ziel**.

   b. Klicken Sie im unteren Fensterbereich auf **Benutzerkennwort eingeben**.

   c. Geben Sie im anschließend angezeigten Fenster die Authentifizierungsmethode für den Benutzer an.

   d. Klicken Sie auf **Übernehmen**, um das Fenster **Kennwort ändern** zu schließen.

6. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

   Der Benutzer wird zur Gruppe hinzugefügt. Wenn es sich um die einzige Gruppenzuweisung handelt, kann sich der Benutzer nun bei den Endpoint Encryption Geräten anmelden.

Symbole für Suchergebnisse hinzufügen/entfernen

Zentrale Symbole	Beschreibung
	Fügt ein einzelnes ausgewähltes Element zum Feld **Ziel** hinzu.

Zentrale Symbole	Beschreibung
	Fügt alle basierend auf Suchkriterien gefundenen Elemente zum Feld **Ziel** hinzu.
	Entfernt ein einzelnes ausgewähltes Element aus dem Feld **Ziel**.
	Entfernt alle Elemente aus dem Feld **Ziel**.

Standardgruppe eines Benutzers ändern

Endpoint Encryption Benutzer können einer beliebigen Anzahl von Gruppen angehören, während Endpoint Encryption Geräte nur jeweils einer Gruppe angehören können. Bei der Standardgruppe handelt es sich um eine Gruppe, die die Richtlinien des Benutzers steuert. Bei der ersten unter "Gruppenmitgliedschaft" aufgeführten Gruppe handelt es sich um die Standardgruppe für den Benutzer.

Hinweis

Der Benutzer muss dazu berechtigt sein, in die Standardgruppe zu installieren. Weitere Informationen finden Sie unter *Benutzer das Installieren in eine Gruppe erlauben auf Seite 11-17*.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie dann **Gruppen auflisten** aus.

   Die Liste **Gruppenmitgliedschaft** wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie dann **An den Anfang verschieben** aus.

Die Standardgruppe des Benutzers wird geändert.

Benutzer das Installieren in eine Gruppe erlauben

Wenn Sie einem Benutzer erlauben, in eine Gruppe zu installieren, ist dieser Benutzer in der Lage, Endpoint Encryption Geräte in eine Gruppe zu installieren, bei der er ein Mitglied ist. Dabei muss dieser Benutzer nicht über die zusätzlichen Berechtigungen einer Administrator- oder Authentifiziererrolle verfügen.

Hinweis

Die Standardeinstellung lautet **Benutzer das Installieren in diese Gruppe nicht erlauben**.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie dann **Gruppen auflisten** aus.

   Die Liste **Gruppenmitgliedschaft** wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer das Installieren in diese Gruppe erlauben** aus.

   Der Benutzer kann jetzt Geräte in diese Gruppe installieren.

Benutzer aus einer Gruppe entfernen

Warnung!

Bevor Sie einen Gruppenadministrator oder ein Gruppenauthentifiziererkonto entfernen, weisen Sie diese Rolle einem anderen Benutzerkonto zu. Andernfalls können nur der Unternehmensadministrator oder der Unternehmensauthentifizierer Änderungen an der Gruppe vornehmen.

Wenn Sie einen Benutzer aus einer Gruppe entfernen, kann der Benutzer nicht mehr auf Endpoint Encryption Geräte zugreifen, die dieser Gruppe zugeordnet sind. Bevor Sie Endpoint Encryption Benutzer entfernen, sollten Sie sich vergewissern, dass die Benutzer ihre Daten gesichert und entschlüsselt haben.

Prozedur

1. Erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Um den Benutzer ebenfalls vom Unternehmen zu entfernen, wählen Sie **Von Unternehmen entfernen**.

   Hinweis

   Beim Entfernen eines Benutzers vom Unternehmen wird der Benutzer ebenfalls aus allen Gruppen und Untergruppen entfernt.
4. Klicken Sie auf **Ja**.

   Der Benutzer wird entfernt.

Alle Benutzer aus einer Gruppe entfernen

Warnung!

Bevor Sie einen Gruppenadministrator oder ein Gruppenauthentifiziererkonto entfernen, weisen Sie diese Rolle einem anderen Benutzer zu. Andernfalls können nur der Unternehmensadministrator und der Unternehmensauthentifizierer Änderungen auf Gruppenebene vornehmen.

Prozedur

1. Erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Alle Benutzer entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Um alle Benutzer ebenfalls vom Unternehmen zu entfernen, wählen Sie **Von Unternehmen entfernen**.

   Hinweis

   Beim Entfernen eines Benutzers vom Unternehmen wird der Benutzer ebenfalls aus allen Gruppen und Untergruppen entfernt.
4. Klicken Sie auf **Ja**.

Gelöschtes Benutzer wiederherstellen

In Umgebungen mit Control Manager und PolicyServer MMC können Sie gelöschte Endpoint Encryption Benutzer mit dem Papierkorb-Knoten von PolicyServer MMC wiederherstellen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie den **Papierkorb**.
3. Öffnen Sie **Gelöschte Benutzer**.

   Im rechten Fenster werden alle gelöschten Benutzer geladen.
4. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto, und wählen Sie anschließend **Benutzer wiederherstellen**.

   Der Benutzer wird wieder zum Unternehmen hinzugefügt, gehört jedoch keiner Richtliniengruppe an.

Arbeiten mit Kennwörtern

Wenn ein Benutzer das Kennwort vergisst oder ein Endpunkt abhanden kommt, kann der Benutzer das Kennwort unter Verwendung der durch die Richtlinien definierten Methoden zurücksetzen. Die folgenden Methoden zum Zurücksetzen von Kennwörtern stehen zur Verfügung:

- Microsoft Windows Active Directory
- Control Manager
- PolicyServer MMC
- Remote-Hilfe
- Selbsthilfe

Bei allen genannten Optionen ist es ggf. erforderlich, die Richtlinie auf Unternehmens- oder Gruppen-/Richtlinienebene festzulegen. Verwenden Sie die Richtlinie "Support-Informationen", um Benutzern Informationen zum Zurücksetzen von Kennwörtern zur Verfügung zu stellen.

Hinweis

Informationen zur Konfiguration der Support-Informationen in Control Manager finden Sie unter *Endpoint Encryption Richtlinieneinstellungen auf Seite 5-14*.

Informationen zur Konfiguration der Support-Informationen in PolicyServer MMC finden Sie unter *Setup für Support-Informationen auf Seite 11-31*.

Unternehmensadministrator-/Authentifiziererkennwort zurücksetzen

Nur Unternehmensadministratoren können ein Unternehmensadministrator-Kennwort zurücksetzen. Ein Authentifizierer mit denselben Gruppenberechtigungen oder mehr kann ein Administrator- oder Authentifiziererkennwort innerhalb dieser Gruppe zurücksetzen.

Tipp

Um dem Verlust von Kennwörtern vorzubeugen, empfiehlt Trend Micro das dauerhafte Vorhandensein von mindestens drei Unternehmensadministratorkonten. Wenn ein Kennwort für ein Unternehmensadministratorkonto verloren geht, rufen Sie die Selbsthilfe auf, um es zurückzusetzen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC mit einem Unternehmensadministratorkonto an.
2. Öffnen Sie **Unternehmen - Benutzer**.
3. Klicken Sie mit der rechten Maustaste auf das Unternehmensadministrator- oder -authentifiziererkonto mit dem verlorenen Kennwort, und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Kennwort ändern** wird angezeigt.
4. Wählen Sie eine Authentifikationsmethode aus.
5. Geben Sie das Kennwort ein (falls erforderlich).

6. Klicken Sie auf **Übernehmen**.

   Das Kontokennwort wird zurückgesetzt.

Hinweis

Die Option **Benutzer muss Kennwort bei nächster Anmeldung ändern** ist nur nach der Aktualisierung der Richtlinien auf dem Agent verfügbar.

Gruppenadministrator-/Authentifiziererkennwort zurücksetzen

Änderungen an Kennwörtern wirken sich nur auf die ausgewählte Gruppe aus. Um die Anzahl der Kennwörter zu reduzieren, weisen Sie Gruppenadministratorkonten nur einer Top-Gruppe zu.

Prozedur

1. Melden Sie sich bei PolicyServer MMC mit einem Gruppenadministratorkonto an.
2. Erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
3. Klicken Sie mit der rechten Maustaste auf das Gruppenadministrator- oder Gruppenauthentifiziererkonto mit dem verlorenen Kennwort, und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Kennwort ändern** wird angezeigt.
4. Wählen Sie eine Authentifikationsmethode aus.
5. Geben Sie das Kennwort ein und bestätigen Sie es (falls erforderlich).
6. Klicken Sie auf **Übernehmen**.

   Das Kontokennwort wird zurückgesetzt.

Hinweis

Die Option **Benutzer muss Kennwort bei nächster Anmeldung ändern** ist nur nach Client-Aktualisierungen verfügbar.

Benutzerkennwörter zurücksetzen

Aktivieren Sie beim Zurücksetzen eines Benutzerkennworts das Kontrollkästchen **Benutzer muss Kennwort bei nächster Anmeldung ändern**, damit ein Benutzer sein Kennwort ändern muss, wenn er sich das nächste Mal anmeldet. Der Benutzer muss sein Kennwort nach der Anmeldung bei einem beliebigen Endpoint Encryption Gerät ändern.

Tipp

Trend Micro empfiehlt die Verwendung der Domänenauthentifizierung.

Auf ein festes Kennwort zurücksetzen

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**, oder erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
2. Wählen Sie die Benutzerkonten im rechten Fensterbereich.

   Hinweis

   Halten Sie die Umschalttaste gedrückt, um mehrere Benutzer auszuwählen. Die Mehrfachauswahl ist nur auf der Gruppenebene möglich.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Kennwort ändern** wird angezeigt.
4. Wählen Sie als **Authentifizierungsmethode** den Eintrag **Festes Kennwort** aus.
5. Geben Sie das Kennwort ein und bestätigen Sie es.

6. Klicken Sie auf **Übernehmen**.

   Nach der erfolgreichen Anmeldung an einem Endpoint Encryption Gerät muss der Benutzer sein Kennwort ändern.

Benutzerkennwort mit Active Directory zurücksetzen

Trend Micro empfiehlt die Verwendung von Active Directory zum Zurücksetzen des Benutzerkennworts, besonders dann, wenn der Benutzer Zugriff auf das Helpdesk des Unternehmens hat, über eine Netzwerkverbindung verfügt oder wenn Windows Single-Sign-On (SSO) aktiviert ist.

Weitere Informationen zum Zurücksetzen eines Domänenbenutzerkennworts mit Active Directory finden Sie im Benutzerhandbuch zum jeweiligen Betriebssystem.

SmartCard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch ein physisches Token zur Bestätigung der Identität des Benutzers. Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- Das Smartcard-Lesegerät ist mit dem Endpunkt verbunden, wobei sich die Smartcard im Lesegerät befindet.
- ActivClient 6.1 ist mit alle Service Packs und Updates installiert.
- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.

Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Hinweis

Smartcard-Authentifizierung kann nur mit PolicyServer MMC konfiguriert werden.

Aktivieren Sie die Smartcard-Authentifizierung für jeden Endpoint Encryption Agent:

- Navigieren Sie für File Encryption zu **Anmelden** > **Kennwort** > **Physischer Token erforderlich**.
- Navigieren Sie für Full Disk Encryption zu **Full Disk Encryption** > **Anmelden** > **Token-Authentifizierung**.

Smartcard-Registrierung

Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Registrieren Sie eine Smartcard, indem Sie eine der folgenden Methoden anwenden:

- Informationen zur Verwendung von Full Disk Encryption Preboot finden Sie unter *Eine Smartcard in Full Disk Encryption Preboot registrieren auf Seite 11-27*.
- Informationen zur Verwendung von PolicyServer MMC finden Sie unter *Smartcard-Authentifizierung in PolicyServer MMC konfigurieren auf Seite 11-25*.

Smartcard-Authentifizierung in PolicyServer MMC konfigurieren

Wenn Sie eine Smartcard registrieren, können sich Benutzer mit der Smartcard-Authentifizierung anmelden. Informationen über die Smartcard-Authentifizierung von Full Disk Encryption Preboot finden Sie unter *File Encryption Smartcard-Authentifizierung auf Seite 13-4*.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Navigieren Sie zu **Full Disk Encryption** > **Anmelden**.
3. Klicken Sie mit der rechten Maustaste auf **Token-Authentifizierung**, und wählen Sie **Aktivieren**.
4. Navigieren Sie zu **Full Disk Encryption** > **Kennwort**.

5. Klicken Sie mit der rechten Maustaste auf **Zulässige Authentifizierungsmethoden**, und wählen Sie anschließend **Eigenschaften**.

   Das Fenster **Richtlinienwert bearbeiten** wird geöffnet.

6. Wählen Sie **PIN**, und klicken Sie anschließend auf **OK**, um die Richtlinienänderung zu bestätigen.

Smartcard-Authentifizierung ist aktiviert.

Smartcard in PolicyServer MMC registrieren

Bevor Sie fortfahren, vergewissern Sie sich, dass die Smartcard-Authentifizierung konfiguriert wurde. Weitere Informationen zur Konfiguration der Smartcard-Authentifizierung finden Sie unter *Smartcard-Authentifizierung in PolicyServer MMC konfigurieren auf Seite 11-25*.

Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Nachdem Sie eine Smartcard-PIN dem Benutzer zugewiesen haben, kann der Benutzer sich direkt beim Full Disk Encryption Agent mit der Smartcard über das Fenster "Smartcard-Authentifizierung" in Full Disk Encryption Preboot anmelden.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Führen Sie die Smartcard in das Lesegerät ein.
3. Verbinden Sie das Lesegerät mit dem PolicyServer Endpunkt.
4. Erweitern Sie die entsprechende Gruppe, und klicken Sie anschließend auf **Benutzer**.
5. Klicken Sie mit der rechten Maustaste auf den Benutzer, und wählen Sie anschließend **Kennwort ändern**.

Das Fenster **Kennwort ändern** wird angezeigt.

6. Wählen Sie im Listenfeld **Authentifizierungsmethode** den Eintrag **Smartcard**.
7. Geben Sie die **PIN** ein, und bestätigen Sie sie.
8. Wählen Sie im Listenfeld **Position auswählen** den Smartcard-Typ.
9. Klicken Sie auf **Übernehmen**, um die Token-Authentifizierung zu bestätigen.
10. Klicken Sie auf **OK**, um die Änderungen am Benutzerkonto zu bestätigen.

Die Smartcard ist für alle Benutzer registriert, die sich in derselben Gruppe wie der ausgewählte Benutzer befinden.

Eine Smartcard in Full Disk Encryption Preboot registrieren

Prozedur

1. Folgen Sie den Anweisungen, um Kennwörter zu ändern, und wählen Sie anschließend **Smartcard**.

   Weitere Informationen finden Sie unter *Benutzerkennwörter zurücksetzen auf Seite 11-23*.
2. Führen Sie die Smartcard in das Lesegerät ein.
3. Verbinden Sie das Lesegerät mit dem Endpunkt.
4. Geben Sie den Benutzernamen und das feste Kennwort ein.
5. Klicken Sie auf **Fortfahren**.
6. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **Fortfahren**.
7. Führen Sie im Fenster **Token registrieren** Folgendes aus:
   a. Geben Sie die neue PIN ein, die Sie vom Gruppen- oder Unternehmensadministrator erhalten haben.
   b. Bestätigen Sie die neue PIN.
   c. Wählen Sie den Typ der Smartcard aus dem Listenfeld **Token** aus.

d. Klicken Sie auf **Fortfahren**, um die Registrierung des Smartcard-Tokens abzuschließen.

Selbsthilfe-Kennwortrücksetzung verwenden

Benutzer, die ihre Kennwörter vergessen haben, können die Selbsthilfe verwenden, ohne die Unterstützung durch das Helpdesk für die Authentifizierung anzufordern. Verwenden Sie die Richtlinien "Anzahl der Fragen" und "Persönliche Herausforderung", um die persönlichen Herausforderungsfragen und die Fragen, die der Benutzer beantworten muss, festzulegen. Selbsthilfefragen werden bei der ersten Benutzerauthentifizierung und wenn Benutzer ihre Kennwörter ändern beantwortet.

Informationen über die Verwendung der Selbsthilfe finden Sie unter *Selbsthilfe auf Seite 2-14*.

Hinweis

Für die Selbsthilfe ist es erforderlich, dass der Endpoint Encryption Agent eine Netzwerkverbindung mit PolicyServer hat.

Prozedur

1. Erweitern Sie **Unternehmen - Richtlinien** oder erweitern Sie die Gruppe und dann **Richtlinien**.
2. Navigieren Sie zu **Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Selbsthilfe**.

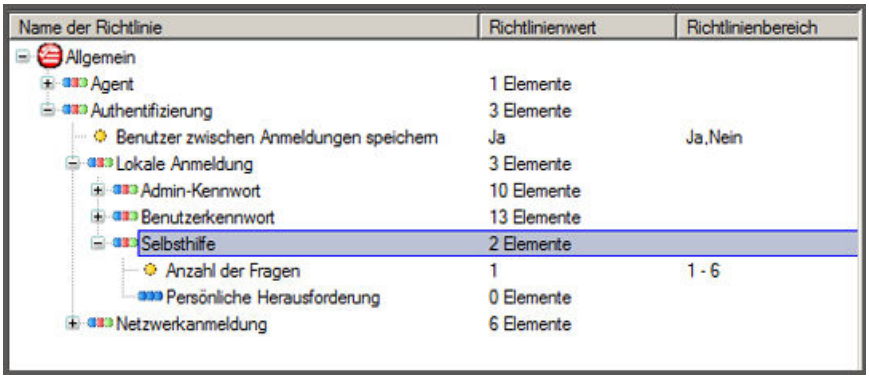


ABBILDUNG 11-5. Selbsthilfe-Richtlinie

3. Öffnen Sie **Anzahl der Fragen**, um die erforderliche Anzahl an Fragen festzulegen, die die Benutzer beantworten müssen.

Warnung!

Legen Sie für **Anzahl der Fragen** keinen Wert größer als 6 fest. Andernfalls können sich Benutzer nicht mit Hilfe der Selbsthilfe authentifizieren.

---

4. Klicken Sie mit der rechten Maustaste auf **Persönliche Herausforderung** und wählen Sie **Hinzufügen** aus, um eine Frage festzulegen, die der Benutzer beantworten muss. Wiederholen Sie diesen Vorgang, bis alle persönlichen Herausforderungsfragen festgelegt sind.

   Der Benutzer wird aufgefordert, die Antworten für die persönlichen Herausforderungsfragen festzulegen, wenn er sich das nächste Mal bei einem Endpoint Encryption Gerät anmeldet.

Unterstützung durch Remote-Hilfe

Mit Hilfe von Remote-Hilfe können Benutzer ein vergessenes Kennwort oder ein gesperrtes Konto zurücksetzen. Jeder Endpoint Encryption Benutzer mit einem gesperrten Konto oder vergessenen Kennwort muss das Kennwort zurücksetzen, bevor er sich wieder bei einem Endpoint Encryption Gerät anmelden kann. Remote-Hilfe

setzt voraus, dass der Benutzer beim Helpdesk eine Herausforderungsantwort anfordert. Für die Remote-Hilfe ist keine Netzwerkverbindung zu PolicyServer erforderlich.

Prozedur

1. Melden Sie sich bei PolicyServer MMC mit einem beliebigen Konto mit Gruppenadministrator-Berechtigungen aus derselben Richtliniengruppe wie der Benutzer an.
2. Fordern Sie den Benutzer auf, vom Endpoint Encryption Agent aus zu **Hilfe** > **Remote-Hilfe** zu navigieren.
3. Fragen Sie den Benutzer nach der **Geräte-ID**.

ABBILDUNG 11-6. Unterstützung durch Remote-Hilfe

4. Öffnen Sie in PolicyServer MMC die Option **Unternehmen - Geräte**, oder erweitern Sie die Gruppe des Benutzers, und öffnen Sie **Geräte**.

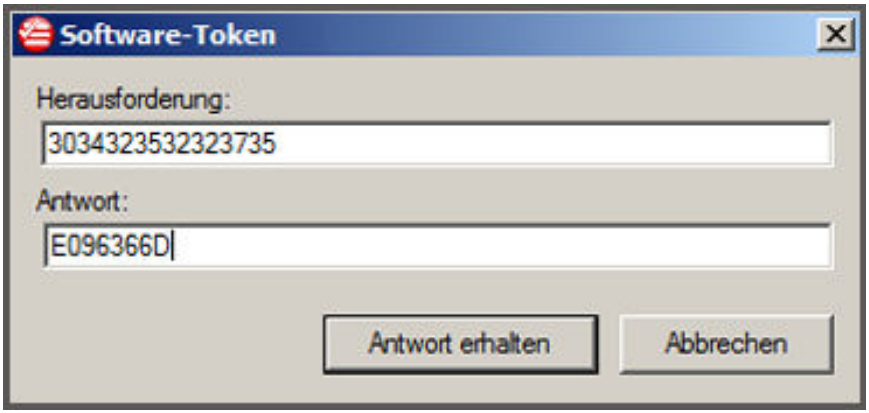
5. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Benutzergerät, und wählen Sie **Software-Token** aus.

   Das Fenster **Soft-Token** wird angezeigt.

6. Fragen Sie den Benutzer nach dem aus 16 Ziffern bestehenden Herausforderungscode, und geben Sie ihn in das Feld **Herausforderung** im Fenster **Software-Token** ein.

7. Klicken Sie auf **Antwort erhalten**.

   Das Feld **Antwort** wird mit einer aus 8 Zeichen bestehenden Zeichenfolge geladen.



8. Teilen Sie dem Benutzer die aus 8 Zeichen bestehende Zeichenfolge über das Feld **Antwort** mit.

9. Der Benutzer gibt die Zeichenfolge im Feld **Antwort** am Endpunkt ein und klickt auf **Anmelden**.

10. Der Benutzer muss ein neues Kennwort eingeben.

Setup für Support-Informationen

Die Richtlinie für Support-Informationen gibt Informationen zum Support-Helpdesk des Unternehmens an. Sie können die Richtlinie für Support-Informationen für jede Gruppe individuell konfigurieren.

Prozedur

1. Melden Sie sich bei PolicyServer MMC mit einem Unternehmensadministrator-/Authentifiziererkonto oder einem Gruppenadministrator-/Authentifiziererkonto innerhalb derselben Richtliniengruppe wie der Benutzer an.
2. Erweitern Sie die Gruppe des Benutzer, und navigieren Sie zu **Richtlinien** > **Full Disk Encryption** > **Anmelden**.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie **Support-Informationen** und wählen Sie **Hinzufügen** aus.
4. Geben Sie die Support-Informationen ein.
5. Klicken Sie auf **OK**.

Remote-Hilfe zum Entsperren von Full Disk Encryption Geräten verwenden

Wichtig

- Durch einen Neustart des Endpoint Encryption Geräts wird der Herausforderungscode geändert.
- Durch eine manuelle Synchronisierung der Richtlinien mit PolicyServer wird der Herausforderungscode ebenfalls geändert.
- Bei Herausforderungscodes und Antwortcodes muss die Groß-/Kleinschreibung nicht berücksichtigt werden.

Prozedur

1. Navigieren Sie in Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Remote-Hilfe**.
2. Übermitteln Sie den **Herausforderungscode** an den Richtlinien-/Gruppenadministrator.

3. Geben Sie den **Antwortcode** ein, den Sie vom Richtlinien-/Gruppenadministrator erhalten haben.

4. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

> **Hinweis**
>
> Wenn für das Konto die Domänenauthentifizierung verwendet wird, startet der Endpunkt direkt in Windows.

5. Geben Sie das neue Kennwort an, bestätigen Sie es und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Mit Remote-Hilfe ein File Encryption Gerät entsperren

Wenn ein Benutzer die Anzahl an Authentifizierungsversuchen überschritten hat und die Remote-Authentifizierung auf Grund von Richtlinien aktiviert ist, sperrt File Encryption die Endpoint Encryption Ordner und benachrichtigt den Benutzer, dass Remote-Hilfe erforderlich ist. Wenn Sie File Encryption über die Remote-Hilfe entsperren möchten, benötigen Sie die Hilfe vom Unternehmensauthentifizierer oder Gruppenauthentifizierer.

> **Hinweis**
>
> Informationen über die Verwendung der Remote-Hilfe finden Sie unter *Remote-Hilfe auf Seite 2-12*.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste, und wählen Sie **Remote-Hilfe**.

Das Fenster **Remote-Hilfe** wird angezeigt.

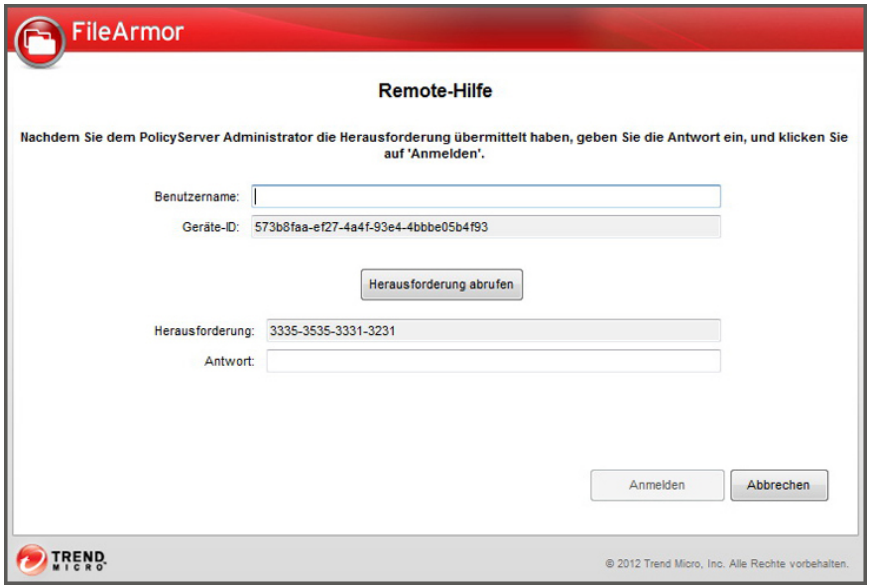


ABBILDUNG 11-7. File Encryption Remote-Hilfe

2. Geben Sie den Benutzernamen an.
3. Klicken Sie auf **Herausforderung abrufen**.
4. Geben Sie die **Antwort** ein, die vom Unternehmens- oder Gruppenauthentifizierer bereitgestellt wurde.
5. Klicken Sie auf **Anmeldung**.

   Der Benutzer wird bei File Encryption authentifiziert und eine Benachrichtigung wird angezeigt.

Kapitel 12

Geräte in PolicyServer MMC

Endpoint Encryption Geräte sind Endpoint Encryption Agents, die bei PolicyServer registriert wurden. Bei der Installation eines Endpoint Encryption Agent wird der Endpunkt automatisch bei PolicyServer als ein Endpoint Encryption Gerät registriert. Da ein bestimmter Endpunkt von mehreren Endpoint Encryption Agents geschützt werden kann, erscheint ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption Geräte auf PolicyServer.

In diesem Kapitel wird erklärt, wie Sie PolicyServer MMC administrieren, um Richtlinien zu verwalten, die sich auf Endpoint Encryption Geräte auswirken, und wie Sie die Datensicherheit mit Hilfe des spezialisierten Widgets für Endpoint Encryption Geräte gewährleisten. In diesem Kapitel wird ebenfalls erklärt, wie Sie gelöschte Endpoint Encryption Geräte wiederherstellen.

Es werden folgende Themen behandelt:

- *Gerät zu einer Gruppe hinzufügen auf Seite 10-13*
- *Gerät aus einer Gruppe entfernen auf Seite 10-14*
- *Gerät aus dem Unternehmen löschen auf Seite 12-5*
- *Software-Token abrufen auf Seite 12-6*
- *Den Wiederherstellungsschlüssel verwenden auf Seite 12-7*
- *Geräteattribute anzeigen auf Seite 12-8*

- *Verzeichnisliste anzeigen auf Seite 12-12*
- *Gruppenmitgliedschaft anzeigen auf Seite 12-12*
- *Gerät auslöschen auf Seite 12-13*
- *Gerät sperren auf Seite 12-14*
- *Ein Gerät zurücksetzen auf Seite 12-14*
- *Gelöschtes Gerät wiederherstellen auf Seite 7-19*

Gerät zu einer Gruppe hinzufügen

Hinweis

Jedes Endpoint Encryption Gerät kann nur einer einzigen Gruppe angehören.

Prozedur

1. Erweitern Sie im linken Fenster die gewünschte Richtliniengruppe und klicken Sie auf **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät hinzufügen** aus.

   Das Fenster **Geräte zu Gruppe hinzufügen** wird angezeigt.

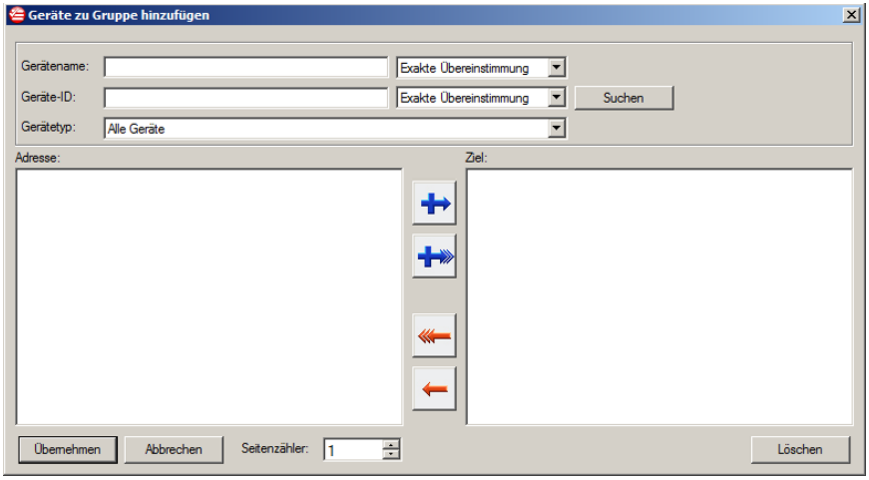


ABBILDUNG 12-1. Fenster Geräte zu Gruppe hinzufügen

3. Geben Sie die Gerätedetails ein, und klicken Sie dann auf **Suchen**.

   Wird eine Übereinstimmung gefunden, werden im Feld **Quelle** die Endpoint Encryption Geräte angezeigt.

4. Wählen Sie die entsprechenden Endpoint Encryption Geräte aus dem Feld **Quelle**, und klicken Sie anschließend auf den **blauen Pfeil**, um sie hinzuzufügen.

   Weitere Informationen zu Suchsymbolen finden Sie unter *Symbole für Suchergebnisse hinzufügen/entfernen auf Seite 11-15*.

5. Klicken Sie auf **Übernehmen**, um das Endpoint Encryption Gerät der ausgewählte Gruppe hinzuzufügen.

   Das Endpoint Encryption Gerät wird der Gruppe hinzugefügt.

Symbole für Suchergebnisse hinzufügen/entfernen

Zentrale Symbole	Beschreibung
	Fügt ein einzelnes ausgewähltes Element zum Feld **Ziel** hinzu.
	Fügt alle basierend auf Suchkriterien gefundenen Elemente zum Feld **Ziel** hinzu.
	Entfernt ein einzelnes ausgewähltes Element aus dem Feld **Ziel**.
	Entfernt alle Elemente aus dem Feld **Ziel**.

Gerät aus einer Gruppe entfernen

Beim Löschen eines Geräts aus einer Gruppe wird das Gerät nur aus der ausgewählten Gruppe entfernt.

Warnung!

Um ein Gerät aus allen Gruppen zu entfernen, entfernen Sie es aus dem Unternehmen. Stellen Sie vor dem Löschen eines Geräts aus dem Unternehmen sicher, dass das Gerät entschlüsselt wurde und alle Endpoint Encryption Agents deinstalliert wurden. Falls Sie dies nicht tun, könnte dies zu irreversiblen Datenverlusten führen.

Prozedur

1. Erweitern Sie die Gruppe, und öffnen Sie dann **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Klicken Sie auf **Ja**.

   Das Gerät wird entfernt.

Gerät aus dem Unternehmen löschen

Wenn Sie ein Endpoint Encryption Gerät aus dem Unternehmen löschen, wird das Gerät auch aus allen Richtliniengruppen entfernt. Das gelöschte Endpoint Encryption Gerät funktioniert, solange die Richtlinien für Konnektivität und Kennwort auf dem Gerät aktuell sind. Die Endpoint Encryption Benutzer können jedoch keine Dateien wiederherstellen, wenn es auf dem Endpoint Encryption Gerät zu einem kritischen Hardwarefehler kommt, nachdem es aus dem Unternehmen entfernt wurde. Um das Risiko zu senken, sollten Sie das Endpoint Encryption Gerät sofort entschlüsseln und die Software für den Endpoint Encryption Agent deinstallieren.

Warnung!

Sorgen Sie dafür, dass das Gerät (Dateien oder Festplatte) entschlüsselt wird, und deinstallieren Sie den Endpoint Encryption Agent, bevor Sie ein Gerät aus dem Unternehmen löschen. Andernfalls besteht die Gefahr von Datenverlusten.

Informationen zum Entfernen eines Geräts aus einer bestimmten Gruppe aber nicht aus dem Unternehmen finden Sie unter *Gerät aus einer Gruppe entfernen auf Seite 10-14*.

Prozedur

1. Deinstallieren Sie den Endpoint Encryption Agent vom Endpunkt.

   Hinweis

   Informationen zur Deinstallation von Endpoint Encryption Agents finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

2. Öffnen Sie **Unternehmen - Geräte**.
3. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät, und wählen Sie **Gerät löschen** aus.
4. Klicken Sie zur Bestätigung auf **Ja**, wenn die Warnmeldung angezeigt wird.

Das Endpoint Encryption Gerät wird aus dem Unternehmen gelöscht.

Hinweis

Informationen darüber, wie Sie das Endpoint Encryption Gerät wieder dem Unternehmen hinzufügen, finden Sie unter *Gelöschtes Gerät wiederherstellen auf Seite 7-19*.

Software-Token abrufen

Wenn Sie ein „Software-Token“ erstellen, wird eine eindeutige Zeichenfolge erstellt, mit deren Hilfe Endpoint Encryption Geräte entsperrt werden können. Auf diese Weise können Sie die Remote-Hilfe für Endpoint Encryption Benutzer ausführen, um vergessene Kennwörter zurückzusetzen.

Informationen über das Zurücksetzen von Kennwörtern oder Entsperren eines Benutzerkontos finden Sie unter *Unterstützung durch Remote-Hilfe auf Seite 11-29*.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie mit der rechten Maustaste auf das Gerät, und wählen Sie **Software-Token**.

   Das Fenster **Software-Token** wird angezeigt.

3. Fragen Sie den Benutzer nach dem aus 16 Ziffern bestehenden Herausforderungscode, und geben Sie ihn in das Feld **Herausforderung** im Fenster **Software-Token** ein.

4. Klicken Sie auf **Antwort erhalten**.

   Das Feld **Antwort** wird mit einer aus 8 Zeichen bestehenden Zeichenfolge geladen.

5. Teilen Sie dem Benutzer die aus 8 Zeichen bestehende Zeichenfolge über das Feld **Antwort** mit.

Das Endpoint Encryption Gerät wird entsprerrt und der Endpoint Encryption Benutzer kann sich am Gerät anmelden.

Den Wiederherstellungsschlüssel verwenden

Wenn Sie einen „Wiederherstellungsschlüssel“ generieren, können Benutzer eine Festplatte entschlüsseln, wenn der Benutzer das ursprüngliche Kennwort oder den ursprünglichen Schlüssel vergessen hat. Der Wiederherstellungsschlüssel ist nur für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker Agents verfügbar, weil diese keine der anderen verfügbaren Wiederherstellungsmethoden in Full Disk Encryption verwenden.

Hinweis

Der Wiederherstellungsschlüssel wird für verschlüsselte Geräte eingesetzt und ist nur als Option verfügbar, wenn die entsprechenden Geräte ausgewählt werden.

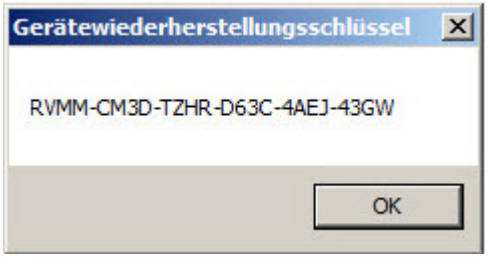
Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf das Gerät, und wählen Sie anschließend **Wiederherstellungsschlüssel**.

   Das Fenster **Wiederherstellungsschlüssel** wird angezeigt.



3. Kopieren Sie den gewünschten Wiederherstellungsschlüssel auf das gesperrte Gerät.

4. Klicken Sie auf **OK**.

Geräteattribute anzeigen

Über **Geräteattribute** zeigen Sie den aktuellen Snapshot des ausgewählten Geräts an.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät, und wählen Sie **Geräteattribute** aus.

   Das Fenster **Geräteattribute** wird angezeigt.

Endpoint Encryption Geräteattribute

In der folgenden Tabelle werden die Endpoint Encryption Geräteattribute beschrieben.

TABELLE 12-1. Endpoint Encryption Geräteattribute

ATTRIBUTNAME	BEISPIEL	BESCHREIBUNG
.NET-Version	2.0.50727.3620	Die Versions- und Build-Nummer für das installierte .NET Framework
Build-Nummer des Common Framework	5.0.0.84	Der Endpoint Encryption Agent verwendet ein Common Framework zur Verschlüsselung. Anhand der Build-Nummer erkennen Sie, ob der Agent aktuell ist
Modell der Festplatte	VMware Virtual IDE	Der Festplattenmodus.
Festplattenname	`\\.\PHYSICALDRIVE0`	Der Name der Festplatte.
Festplattenpartitionen	1	Die Anzahl der Partitionen auf der Festplatte, auf der der Agent installiert ist.

Attributname	Beispiel	Beschreibung
Größe der Festplatte	10733990400	Die Gesamtkapazität der Festplatte (Byte).
Domänenname	WORKGROUP	Die Domäne, zu der der Endpunkt gehört.
Endpunkt-ID	85b1e3e2a3c25d882540ef6e4818c3e4	Die eindeutige ID des Endpunkts, die zur Control Manager Integration verwendet wird.
<Agent> Benutzer	maryjane	Der Benutzername des zuletzt angemeldeten Benutzers.
<Agent> Version	5.0.0.260	Die Versions- und die Build-Nummer für die Agent-Installation.
Host-Name	TREND-4136D2DB3	Der Host-Name des Endpunkts.
IP-Adresse	10.1.152.219	Die IP-Adresse des Endpunkts.
Gebietsschema	Deutsch (Deutschland)	Die Sprache und die Region, für die der Endpunkt konfiguriert wurde.
Computername	TREND-4136D2DB3	Der Computername, den dieser Endpunkt verwendet.
Hersteller	VMware, Inc.	Der Hersteller der Festplatte.
Modell	Virtuelle VMware-Plattform	Das Modell der Festplatte.
Betriebssystem	Microsoft Windows NT 5.1.2600 Service Pack 3	Das Betriebssystem, das auf derselben Festplatte wie der Agent installiert ist.

Attributname	Beispiel	Beschreibung
Name des Betriebssystems	Microsoft Windows XP Professional	Der allgemeine Name des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Service Pack des Betriebssystems	Service Pack 3	Die Nummer des Service-Packs des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Version des Betriebssystems	5.1.2600.196608	Die Versionsnummer des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Partitionsschema	Klassischer MBR	Das Partitionsschema für die Festplatte.
Prozessor	x86 Family 6 Modell 30 Stepping 5, Genuine Intel	Marke und Modell des Prozessors auf dem Endpunkt.
Prozessoranzahl	2	Die Anzahl der Prozessoren im Endpunkt.
Prozessorrevision	1e05	Die Prozessorrevisionsnummer.
Zeitzone	Taipei Standardzeit	Die Zeitzone, in der sich der Endpunkt befindet.
Gesamter physischer Arbeitsspeicher	2.047MB	Die Gesamtmenge des Arbeitsspeichers (RAM), der auf dem Endpunkt installiert oder zugeordnet ist.
Typ	X86-basierter PC	Der Prozessortyp des Endpunkts.

ATTRIBUTNAME	BEISPIEL	BESCHREIBUNG
Windows Benutzername	TREND-4136D2DB3\admin	Der Benutzername des Windows-Kontos, das sich das letzte Mal am Endpunkt angemeldet hat.

Verzeichnisliste anzeigen

Hinweis

Verwenden Sie die Verzeichnisliste, um die Verzeichnisstruktur von KeyArmor-Geräten anzuzeigen. Die Verzeichnisliste ist nur in Umgebungen verfügbar, die von einer früheren PolicyServer Version aktualisiert wurden und in der sich registrierte KeyArmor Geräte befanden.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Verzeichnisliste** aus.

   Das Fenster **Snapshot des Geräteverzeichnisses** wird angezeigt.

Gruppenmitgliedschaft anzeigen

Hinweis

Ein Gerät darf nur zu einer Gruppe gehören.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät, und wählen Sie **Gruppen auflisten** aus.

   Das Fenster **Gruppenmitgliedschaft** wird angezeigt.

Gerät auslöschen

Die Ausführung eines „Auslöschen"-Befehls löscht alle Endpoint Encryption Gerätedaten. Welche Daten gelöscht werden, ist abhängig vom Geltungsbereich der Daten, der vom verbundenen Endpoint Encryption Agent verwaltet wird. Wenn Sie beispielsweise einen „Auslöschen"-Befehl auf ein Full Disk Encryption Gerät ausführen, werden alle Daten vom Endpunkt gelöscht. Führen Sie dagegen einen „Auslöschen"-Befehl auf ein File Encryption Gerät aus, werden alle Dateien und Ordner auf dem lokalen Datenträger und auf den Wechselmedien gelöscht, die vom File Encryption Agent geschützt werden. Der „Auslöschen"-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert.

Warnung!

Das Auslöschen eines Geräts kann nicht rückgängig gemacht werden. Führen Sie eine Datensicherung der gesamten Daten durch, bevor Sie einen Auslöschen-Befehl geben.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät auslöschen** aus.
3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
4. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gerät sperren

Wenn Sie den Befehl „Sperren“ auf das Endpoint Encryption Gerät anwenden, wird der Endpoint Encryption Benutzerzugriff verhindert, bis eine erfolgreiche Authentifizierung für die Remote-Hilfe durchgeführt wurde. Beim Sperren eines Gerät wird der Endpunkt neu gestartet und in einen Status gezwungen, der Remote-Hilfe erfordert. Der Sperren-Befehl wird ausgegeben, wenn der Endpoint Encryption Agent mit PolicyServer kommuniziert.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.
2. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie **Gerät sperren** aus.
3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
4. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Ein Gerät zurücksetzen

Wenn Sie einen „Warmstart“-Befehl geben, wird der Endpunkt neu gestartet. Der Befehl wird das nächste Mal ausgeführt, wenn der Agent mit PolicyServer kommuniziert.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

   Alle Geräte im Unternehmen oder in einer Gruppe werden im rechten Fensterbereich angezeigt.

2. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie **Warmstart** aus.

3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

4. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gelöschtes Gerät wiederherstellen

Im Umgebungen mit Control Manager und PolicyServer MMC können Sie gelöschte Endpoint Encryption Geräte mit dem Papierkorb-Knoten von PolicyServer MMC wiederherstellen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.

2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.

3. Erweitern Sie den **Papierkorb**.

4. Öffnen Sie **Gelöschte Geräte**.

   Im rechten Fensterbereich werden alle gelöschten Endpoint Encryption Geräte angezeigt.

5. Klicken Sie mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie anschließend **Gerät wiederherstellen**.

Das Endpoint Encryption Gerät wird wieder zum Unternehmen hinzugefügt, gehört jedoch keiner Richtliniengruppe an.

Teil IV

Verwaltung von Endpoint Encryption Agents

Kapitel 13

File Encryption

File Encryption schützt einzelne Dateien und Ordner auf lokalen Festplatten und auf Wechselmedien (USB-Laufwerken). Sie können Richtlinien festlegen, die angeben, welche Ordner und Laufwerke auf dem Gerät verschlüsselt sind, und die Richtlinien zu verschlüsselten Daten auf Wechselmedien festlegen. Verschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

File Encryption kann auch verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, wodurch Sie in der Lage sind, Zugriffsrichtlinien für ein File Encryption Gerät und separate Richtlinien für den Zugriff auf bestimmte Dateien festzulegen. Dies ist in Umgebungen nützlich, in denen mehrere Benutzer auf einen Endpunkt zugreifen.

Es werden folgende Themen behandelt:

- *Info über die File Encryption auf Seite 13-2*
- *File Encryption Authentifizierung auf Seite 13-2*
- *File Encryption Agent - Menü auf Seite 13-11*
- *File Encryption - Kontextmenü auf Seite 13-15*
- *File Encryption Archivverschlüsselung auf Seite 13-16*
- *File Encryption – Archivieren und brennen auf Seite 13-21*
- *Funktion "Sicheres Löschen" von File Encryption verwenden auf Seite 13-22*

Info über die File Encryption

Der Trend Micro File Encryption Agent setzt AES-Verschlüsselung zum Schutz von Daten ein, die zwischen den Endpoint Encryption Benutzern ausgetauscht wurden bzw. die auf Wechseldatenträgern oder auf Netzwerkressourcen gespeichert sind. File Encryption kann ferner verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, Sie können Zugriffsrichtlinien für den File Encryption Agent festlegen und anschließend separate Richtlinien zum Zugriff auf bestimmte Dateien anlegen. Diese Funktion ist in Umgebungen nützlich, in denen mehrere Benutzer auf denselben Endpunkt zugreifen. Verschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

Sie können mit Trend Micro PolicyServer angeben, welche Dateien und Ordner verschlüsselt werden sollen, sowie die Richtlinien zum Verschlüsseln der Wechseldatenträger festlegen.

Endbenutzer sind ebenfalls in der Lage, File Encryption flexibel lokal zu verwalten, indem individuelle Dateien, Ordner oder Wechseldatenträger umgehend verschlüsselt werden. Benutzer sind so in der Lage, auch auf Geschäftsreisen Daten sicher zu schützen.

File Encryption Authentifizierung

In diesem Abschnitt wird erklärt, wie Sie sich bei File Encryption authentifizieren und das Produkt verwenden. Alle Authentifizierungsmethoden für Endpoint Encryption sind in File Encryption verfügbar.

Hinweis

Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode auf Seite 2-7*.

Erstmalige Authentifizierung von File Encryption

Wenn File Encryption zum ersten Mal gestartet wird, ist eine Authentifizierung erforderlich, um PolicyServer zu identifizieren. Die Standardmethode ist die

Authentifizierung mit festem Kennwort. Weitere Optionen hängen von den Richtlinieneinstellungen ab.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste, und wählen Sie **Registrieren**.
2. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein.
3. Geben Sie die IP-Adresse (oder den Host-Namen) sowie das Unternehmen ein.
4. Klicken Sie auf **OK**.

   Das Fenster **Kennwort ändern** wird angezeigt.
5. Wählen Sie die gewünschte Authentifizierung aus dem Listenfeld aus.
6. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **OK**.

Hinweis

Ohne Authentifizierung bei File Encryption wird der Zugriff auf Dateien und Wechselmedien verweigert.

File Encryption Domänenauthentifizierung

Stellen Sie für die Domänenauthentifizierung mit SSO (Single Sign-On) sicher, dass die folgenden Voraussetzungen erfüllt werden:

- Der Benutzer gehört zu einer Richtliniengruppe mit aktivierter Domänenauthentifizierung.
- Vergewissern Sie sich, dass der Host-Name und der Domänenname ordnungsgemäß konfiguriert wurden.
- PolicyServer und alle Endpoint Encryption Geräte, die die Domänenauthentifizierung verwenden, befinden sich in derselben Domäne.

- Das Benutzerkonto wird in Active Directory und PolicyServer konfiguriert. Der Benutzername muss genau übereinstimmen, auch hinsichtlich der Groß- und Kleinschreibung.

Hinweis

Informationen zur Konfiguration der Richtlinien für die Domänenauthentifizierung für SSO finden Sie unter *Regeln der Domänenauthentifizierungsrichtlinie auf Seite 2-11*.

Authentifizierung mit Domänenauthentifizierung durchführen

Prozedur

1. Rufen Sie PolicyServer MMC auf, und navigieren Sie zur folgenden Richtlinienposition:

   File Encryption > **Anmelden** > **Zulässige Authentifizierungsmethoden**

2. Wählen Sie **Domänenauthentifizierung** als Authentifizierungstyp.
3. Geben Sie den Benutzernamen und das Kennwort für das Domänenkonto ein.
4. Klicken Sie auf **OK**.

Hinweis

- Die Domänenauthentifizierung kann nicht mit einer Smartcard-PIN verwendet werden.
- Die Remote-Hilfe ist für Domänenbenutzer verfügbar. Das Domänenkennwort muss allerdings in Active Directory zurückgesetzt werden, wenn es vergessen wird.

File Encryption Smartcard-Authentifizierung

Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- Aktivieren Sie die File Encryption Richtlinie unter **Anmelden** > **Kennwort** > **Physischer Token erforderlich**.
- Das Smartcard-Lesegerät ist mit dem Endpunkt verbunden und die Smartcard ist eingelegt.

Hinweis

File Encryption unterstützt nur CASC- und PIC-Smartcards.

- ActivClient 6.1 muss mit allen Service Packs und Updates installiert sein.
- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.

Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Authentifizierung mit einer Smartcard durchführen

Die File Encryption Smartcard-Authentifizierung ist nur verfügbar, wenn die entsprechende Richtlinie aktiviert ist.

Hinweis

File Encryption unterstützt nur CASC- und PIC-Smartcards.

Prozedur

1. Rufen Sie PolicyServer MMC auf, und navigieren Sie zur folgenden Richtlinienposition:

   File Encryption > **Anmelden** > **Zulässige Authentifizierungsmethoden**

2. Öffnen Sie File Encryption auf dem Endpoint Encryption Gerät, und wählen Sie **Smartcard** aus dem Listenfeld für die Authentifizierung.
3. Geben Sie den Benutzernamen an.

4. Geben Sie die Smartcard-PIN oder das feste Kennwort an (falls zutreffend).
5. Klicken Sie auf **OK**.

File Encryption ColorCode-Authentifizierung

Die File Encryption ColorCode-Authentifizierung ist nur verfügbar, wenn die entsprechende Richtlinie aktiviert ist.

Prozedur

1. Rufen Sie PolicyServer MMC auf, und navigieren Sie zur folgenden Richtlinienposition:

   Gruppenname > **Richtlinien** > **File Encryption** > **Anmelden** > **Zulässige Authentifizierungsmethoden**

2. Wählen Sie **ColorCode** aus dem Authentifizierungs-Listenfeld aus.
3. Geben Sie eine eindeutige ColorCode-Kombination ein.
4. Klicken Sie auf **OK**.

File Encryption PIN-Authentifizierung

Die File Encryption PIN-Authentifizierung ist nur verfügbar, wenn die entsprechende Richtlinie aktiviert ist.

Prozedur

1. Rufen Sie PolicyServer MMC auf, und navigieren Sie zur folgenden Richtlinienposition:

   Gruppenname > **Richtlinien** > **File Encryption** > **Anmelden** > **Zulässige Authentifizierungsmethoden**

2. Wählen Sie **PIN** aus dem Authentifizierungs-Listenfeld aus.

3. Geben Sie die PIN-Kombination an.
4. Klicken Sie auf **OK**.

Kennwort in File Encryption ändern

Um das Kennwort zu ändern, muss der Benutzer sich mit der Kontorolle "Benutzer" bei File Encryption authentifizieren. Der Benutzer kann anschließend das Kennwort mit einer der Authentifizierungsmethoden ändern, die von der Richtlinie zugelassen werden. Sie können mit PolicyServer MMC die Richtlinie verwalten:

Gruppenname > Richtlinien > File Encryption > Anmelden > Zulässige Authentifizierungsmethoden

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste, und wählen Sie **Kennwort ändern**.
2. Geben Sie das Kennwort ein.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie eine verfügbare Authentifizierungsmethode.
5. Geben Sie das neue Kennwort an, und bestätigen Sie es.
6. Klicken Sie auf **OK**.

   Das Kennwort wird aktualisiert und eine Bestätigungsmeldung wird angezeigt.

Erzwungene Kennwortzurücksetzung

File Encryption verhindert den unberechtigten Zugriff auf verschlüsselte Dateien und Ordner, indem geschützte Dateien gesperrt werden, wenn zu viele erfolglose Authentifizierungsversuche durchgeführt werden oder wenn für eine bestimmte Dauer keine Kommunikation zwischen Endpunkt und dem PolicyServer erfolgte. Auf Grund der Richtlinien-Konfiguration sperrt File Encryption den Benutzer für den Zugriff oder

aktiviert eine Zeitverzögerung, bevor Authentifizierungsversuche durchgeführt werden können.

Mit Remote-Hilfe ein File Encryption Gerät entsperren

Wenn ein Benutzer die Anzahl an Authentifizierungsversuchen überschritten hat und die Remote-Authentifizierung auf Grund von Richtlinien aktiviert ist, sperrt File Encryption die Endpoint Encryption Ordner und benachrichtigt den Benutzer, dass Remote-Hilfe erforderlich ist. Wenn Sie File Encryption über die Remote-Hilfe entsperren möchten, benötigen Sie die Hilfe vom Unternehmensauthentifizierer oder Gruppenauthentifizierer.

Hinweis

Informationen über die Verwendung der Remote-Hilfe finden Sie unter *Remote-Hilfe auf Seite 2-12*.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das File Encryption Symbol in der Task-Leiste, und wählen Sie **Remote-Hilfe**.

Das Fenster **Remote-Hilfe** wird angezeigt.

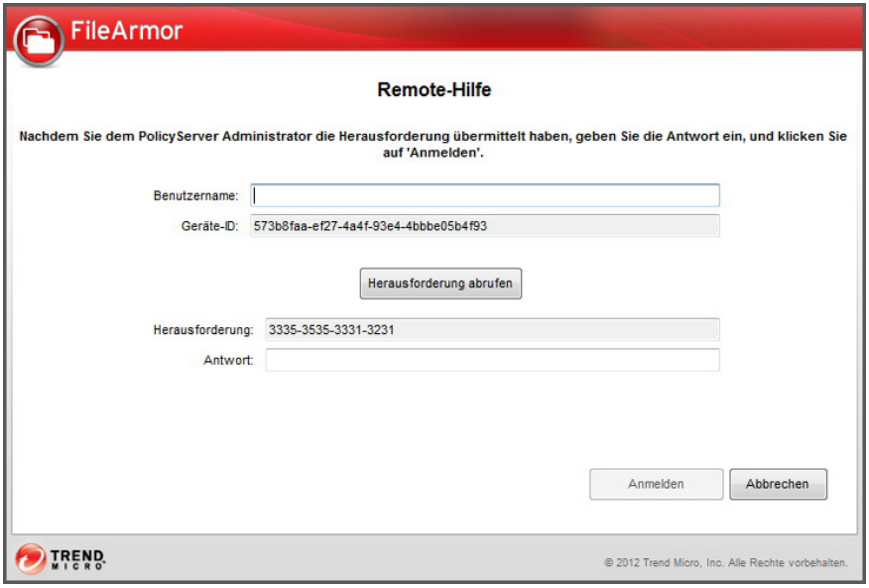


ABBILDUNG 13-1. File Encryption Remote-Hilfe

2. Geben Sie den Benutzernamen an.
3. Klicken Sie auf **Herausforderung abrufen**.
4. Geben Sie die **Antwort** ein, die vom Unternehmens- oder Gruppenauthentifizierer bereitgestellt wurde.
5. Klicken Sie auf **Anmeldung**.

   Der Benutzer wird bei File Encryption authentifiziert und eine Benachrichtigung wird angezeigt.

Richtlinienregeln für Endpoint Encryption Geräte

In der folgenden Tabelle werden die Regeln der Sicherheitsrichtlinie für verlorene oder gestohlene Endpoint Encryption Geräte beschrieben. Abhängig von den

Richtlinieneinstellungen wird nach zu vielen aufeinanderfolgenden erfolglosen Authentifizierungsversuchen an den Endpoint Encryption Geräten der nächste Authentifizierungsversuch verzögert, das Endpoint Encryption Gerät wird gesperrt oder alle Daten, die vom jeweiligen Endpoint Encryption Agent kontrolliert werden, werden gelöscht.

TABELLE 13-1. Optionen zur Gerätesicherheit

SICHERHEITSOPTION	BESCHREIBUNG
Zeitverzögerung	Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen sperrt PolicyServer vorübergehend das Endpoint Encryption Gerät und benachrichtigt den Endpoint Encryption Benutzer diesbezüglich. Während der Zeitverzögerung ist die Möglichkeit zur Authentifizierung oder Kennwortzurücksetzung deaktiviert. Die Dauer der Zeitverzögerung wird von der Richtlinie bestimmt. Nach Ablauf der Zeitverzögerung ist der Benutzer wieder berechtigt, sich zu authentifizieren. **Hinweis** Der Endpoint Encryption Benutzer kann die Selbsthilfe- oder Remote-Hilfe-Authentifizierung verwenden, wenn er nicht bis zum Ablauf der Zeitverzögerung warten will.
Remote-Authentifizierung erforderlich	Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen sperrt PolicyServer vorübergehend das Endpoint Encryption Gerät, bis sich der Endpoint Encryption Benutzer an den technischen Support zur Durchführung einer Remote-Hilfe-Authentifizierung wendet. **Hinweis** Weitere Informationen finden Sie unter *Remote-Hilfe auf Seite 2-12*.

SICHERHEITSOPTION	BESCHREIBUNG
Gerät wird gelöscht	Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen löscht PolicyServer alle Daten, die vom jeweiligen Endpoint Encryption Agent kontrolliert werden. Wenn beispielsweise ein Full Disk Encryption Gerät "gelöscht" wird, werden alle Daten vom Endpunkt gelöscht, während beim Löschen eines File Encryption Geräts alle Dateien und Ordner auf der lokalen Festplatte oder auf den Wechselmedien gelöscht werden, die vom File Encryption Agent geschützt werden. **Warnung!** Der Endpoint Encryption Benutzer kann die gelöschten Daten nicht wiederherstellen.

File Encryption Agent - Menü

Klicken Sie in der Task-Leiste auf das File Encryption-Symbol (), um auf den File Encryption Agent zuzugreifen. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol, um die Menüelemente anzuzeigen. In der folgenden Tabelle werden die verfügbaren Menüoptionen beschrieben.

TABELLE 13-2. Menüoptionen für File Encryption Agent

MENÜELEMENT	FUNKTION
Registrieren	Dient der erstmaligen Benutzerregistrierung von File Encryption beim PolicyServer. Weitere Informationen finden Sie unter *Erstmalige Authentifizierung von File Encryption auf Seite 13-2*.
Anmelden/Abmelden	Dient der Authentifizierung mit PolicyServer.
Kennwort ändern	Erlaubt Benutzern, ihre Kennwörter zu ändern. Weitere Informationen finden Sie unter *Kennwort in File Encryption ändern auf Seite 13-7*.

MENÜELEMENT	FUNKTION
Remote-Hilfe	Sie können mit der Remote-Hilfe File Encryption zur Authentifizierung entsperren, wenn der Benutzer das Endpoint Encryption Kennwort vergessen hat, es zu viele erfolglose Authentifizierungsversuche gab oder das Endpoint Encryption Gerät während eines bestimmten Zeitraums nicht mit dem PolicyServer kommuniziert hat. Weitere Informationen finden Sie unter *Erzwungene Kennwortzurücksetzung auf Seite 13-7*.
Mit PolicyServer synchronisieren	Laden Sie Richtlinien-Updates manuell vom PolicyServer herunter. Weitere Informationen finden Sie unter *Richtlinien mit PolicyServer synchronisieren auf Seite 13-12*.
Offline-Dateien mit PolicyServer synchronisieren	Über die Synchronisierung mit PolicyServer Offline-Dateien mit Hilfe einer Importdatei anstelle der direkten Kommunikation mit PolicyServer können neue Sicherheitsrichtlinien durchgesetzt werden. Weitere Informationen finden Sie unter *Richtlinien mit PolicyServer Offline-Dateien synchronisieren auf Seite 13-13*.
Benachrichtigung verbergen	Schaltet alle File Encryption Benachrichtigungen aus.
Info über die File Encryption	Zeigt File Encryption Informationen an, einschließlich der Version, der letzten Synchronisierung und des authentifizierten Benutzers.
Schließen	Entfernt das File Encryption Task-Leistensymbol vorübergehend.

Richtlinien mit PolicyServer synchronisieren

File Encryption Agents können neue File Encryption Richtlinien mit Hilfe der Option **Mit PolicyServer synchronisieren** im File Encryption Task-Leistensymbol manuell herunterladen.

Hinweis

File Encryption Agents können Richtlinien ohne Benutzerauthentifizierung synchronisieren.

Wenn eine Netzwerkverbindung oder ein PolicyServer nicht verfügbar ist, wird der Fehler **Synchronisierung mit Server konnte nicht durchgeführt werden** angezeigt.

Automatische Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Endpoint Encryption Agents und PolicyServer einleiten.

- Nachdem das Betriebssystem geladen wird und der Dienst des Endpoint Encryption Agent startet

  Hinweis

  Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- Wenn Full Disk Encryption Preboot startet (nur Full Disk Encryption)
- Die Zeitdauer der Richtlinie **Synchronisierungsintervall** läuft ab

Öffnen Sie das Fenster **Info über**, um Endpoint Encryption Agent anzuweisen, die Richtlinien manuell zu synchronisieren.

Hinweis

Aktionen für Endpoint Encryption Geräte werden eingeleitet, nachdem der Endpoint Encryption Agent Richtlinien-Updates erhält.

Richtlinien mit PolicyServer Offline-Dateien synchronisieren

Offline-Updates arbeiten mit File Encryption 3.0.13.2447 oder einer höheren Version und neuerdings mit x64-Installationen von File Encryption. Wenn das Update generiert

wird, werden alle bestehenden Benutzerkennwörter vom Offline-Update durch das neue feste Kennwort ersetzt.

Beim Update werden Benutzerkennwörter nicht durch synchronisierte Kennwörter ersetzt, um dieselbe Funktionalität der verwalteten Geräte zu gewährleisten.

Zum Hinzufügen eines Benutzers zu einem Offline File Encryption Gerät ist ein festes Kennwort erforderlich. Der Offline-Prozess generiert die folgenden zwei Dateien:

PolicyServer wechseln

Aktualisieren Sie über das Menü **Info** von File Encryption den PolicyServer, der die Richtlinien verwaltet.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol für File Encryption, und wählen Sie anschließend **Info über File Encryption**.

   Die Fenster **Info** wird angezeigt.

2. Klicken Sie auf **PolicyServer bearbeiten**.

3. Geben Sie die IP-Adresse oder den Host-Namen für den neuen PolicyServer ein.

4. Klicken Sie auf **OK**.

   File Encryption wird nun vom neuen PolicyServer verwaltet.

File Encryption - Kontextmenü

Benutzer können eine Datei verschlüsseln, indem sie mit der rechten Maustaste auf die Datei klicken und eine Verschlüsselungsoption auswählen. Die folgende Abbildung zeigt einige der verfügbaren Optionen.

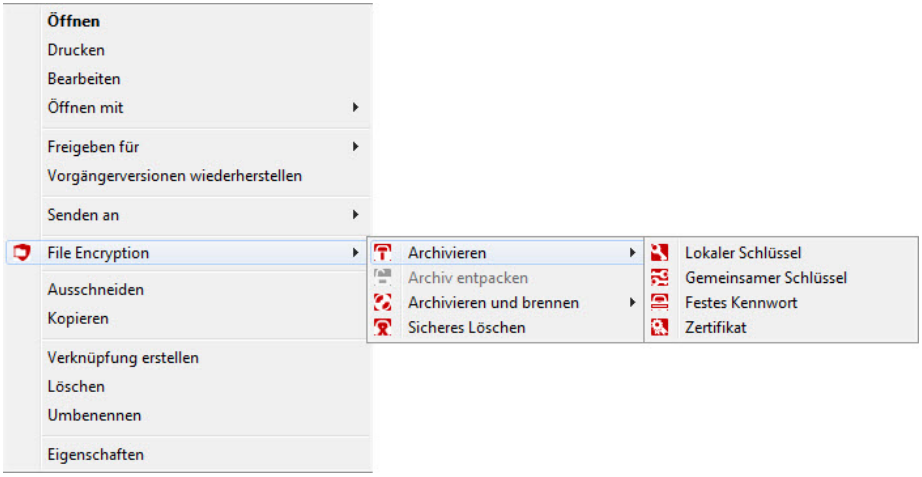


ABBILDUNG 13-2. File Encryption - Kontextmenü

Die folgende Tabelle soll Ihnen helfen, die verfügbaren Menüoptionen zu verstehen.

TABELLE 13-3. File Encryption Optionen im Kontextmenü

MENÜOPTION	BESCHREIBUNG
Archivieren	Erstellen Sie eine verschlüsselte Kopie der angegebenen Datei.
Archiv entpacken	Öffnet ein zuvor erstelltes Archiv.
Archivieren und brennen	Erstellen Sie eine verschlüsselte Kopie der angegebenen Datei und schreiben Sie diese auf eine CD/DVD.
Sicheres Löschen	Sie können die ausgewählten Dateien und die Dateihistorie auf dem File Encryption Gerät sicher löschen.

File Encryption Archivverschlüsselung

File Encryption verschlüsselt Dateien auf Grundlage von Richtlinien, die lokal definiert sind, oder Richtlinien, die von PolicyServer definiert wurden. Die Verschlüsselungsmethode hängt von den Bedürfnissen des Benutzers für den Dateizugriff und von der gewünschten Sicherheitsstufe ab.

Um Dateien automatisch zu verschlüsseln, speichern Sie sie an folgenden Speicherorten:

- Ein Ordner auf dem File Encryption Gerät
- Ein Ordner auf einem Wechselmedium
- Ein vollständig verschlüsselter Wechseldatenträger

File Encryption Verschlüsselung mit lokalem Schlüsseln

Die Auswahl der Funktion "Lokaler Schlüssel" ermöglicht einem Benutzer, Dateien zu verschlüsseln, die nur dieser Benutzer anzeigen kann. Der Zugriff auf lokale Schlüsseldateien kann nur auf einem File Encryption Gerät von dem Benutzer erfolgen, der sie erstellt hat.

Die Richtlinien sind verfügbar unter:

- In Control Manager: Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**, wählen Sie die Richtlinie, und ändern Sie dann die **allgemeinen** Richtlinienregeln. Weitere Informationen finden Sie unter *Allgemeine Regeln für Richtlinien konfigurieren auf Seite 3-23*.
- In PolicyServer MMC: Aktivieren Sie unter **File Encryption** > **Verschlüsselung** > **Zulässige Verschlüsselungsmethode** die Option **Eindeutiger Schlüssel des Benutzers**.

Hinweis

File Encryption erstellt bei der Verschlüsselung einer Datei eine neue Datei. Die Originaldatei verbleibt unverschlüsselt an ihrem ursprünglichen Speicherort.

Warnung!

Je nach Windows Betriebssystem kann ein Benutzer den Inhalt von Ordnern bei einem Benutzerwechsel ohne einen Neustart von Windows anzeigen. Während Dateinamen und Ordnerinhalte angezeigt werden können, ist der Dateiinhalt nicht verfügbar. Dies liegt daran, dass das Windows Betriebssystem die Dateistruktur für die Schnellsuche zwischenspeichert.

Lokale Schlüssel erstellen

Prozedur

- Klicken Sie mit der rechten Maustaste auf die gewünschte Datei, und navigieren Sie anschließend zu **File Encryption** > **Archivieren** > **Lokaler Schlüssel**.

  Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

File Encryption Verschlüsselung mit gemeinsamem Schlüssel

Verschlüsseln Sie mit der Funktion "Gemeinsamer Schlüssel" Dateien, die nur zum Zugriff durch Mitglieder derselben Richtliniengruppe vorgesehen sind.

Die Richtlinien sind verfügbar unter:

- In Control Manager: Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**, wählen Sie die Richtlinie, und ändern Sie dann die **allgemeinen** Richtlinienregeln. Weitere Informationen finden Sie unter *Allgemeine Regeln für Richtlinien konfigurieren auf Seite 3-23*.

- In PolicyServer MMC: Aktivieren Sie unter **File Encryption** > **Verschlüsselung** > **Zulässige Verschlüsselungsmethode** die Option **Gruppenschlüssel**.

Hinweis

Damit ein File Encryption Benutzer verschlüsselte Dateien in PolicyServer Enterprise anzeigen kann, legen Sie **Verwendeter Verschlüsselungsschlüssel** auf **Unternehmensschlüssel** fest.

Hinweis

File Encryption erstellt bei der Verschlüsselung einer Datei eine neue Datei. Die Originaldatei verbleibt unverschlüsselt an ihrem ursprünglichen Speicherort.

Warnung!

Je nach Konfiguration der Windows Berechtigungen kann ein Benutzer den verschlüsselten Inhalt von Ordnern bei Benutzerwechseln ohne einen Neustart von Windows anzeigen. Während die Dateinamen und Ordnerinhalte angezeigt werden können, ist der Dateiinhalt nicht verfügbar. Dies liegt daran, dass das Windows Betriebssystem die Dateistruktur für die Schnellsuche zwischenspeichert.

Gemeinsame Schlüssel erstellen

Prozedur

- Klicken Sie mit der rechten Maustaste auf die gewünschte Datei, und navigieren Sie anschließend zu **File Encryption** > **Archivieren** > **Gemeinsamer Schlüssel**.

  Die ursprünglichen Dateien oder Ordner werden nicht geändert und können beibehalten oder gelöscht werden.

File Encryption Entschlüsselung mit festem Kennwort

File Encryption kann mit einem festen Kennwort verschlüsselte Dateien erstellen. Benutzer können optional festlegen, dass sich die Datei selbstextrahiert, so dass der Empfänger File Encryption nicht benötigt, um die Datei zu entschlüsseln.

Hinweis

- Für die Kennwortwiederherstellung bei selbstextrahierenden Dateien steht keine Funktion zur Verfügung. Wenn ein Kennwort vergessen wird, kann die verschlüsselte Datei nicht wiederhergestellt werden.
- Auf Grund einer Einschränkung von Windows dürfen ausführbare (selbstextrahierende) Dateien nicht größer als 2 GB sein.

Einen festen Kennwortschlüssel erstellen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die gewünschte Datei, und navigieren Sie anschließend zu **File Encryption** > **Archivieren** > **Festes Kennwort**.
2. Geben Sie das neue Kennwort an, und bestätigen Sie es.
3. Wählen Sie bei Bedarf die optionale Option **Verschlüsselte Daten als selbstextrahierendes Archiv ausgeben**.
4. Klicken Sie auf **OK**.

   Die Datei wird verschlüsselt.
5. Gehen Sie wie folgt vor, um die Datei zu entschlüsseln:
   a. Doppelklicken Sie auf die Datei.
   b. Geben Sie das Archivkennwort ein.
   c. Klicken Sie auf **OK**.
6. Führen Sie für selbstextrahierende Archive Folgendes aus:
   a. Doppelklicken Sie auf die Datei.
   b. Geben Sie das Archivkennwort ein.
   c. Wählen Sie den Speicherort, an dem die Dateien extrahiert werden sollen.
   d. Wählen Sie, ob das Zielverzeichnis nach der Extrahierung geöffnet oder bereits vorhandene Dateien überschrieben werden sollen.

e. Klicken Sie auf **Fortfahren**.

Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

File Encryption Verschlüsselung mit digitalem Zertifikat

File Encryption kann Dateien mit digitalen Zertifikaten (Smartcards) aus dem Windows Zertifikatsspeicher verschlüsseln.

Digitalen Zertifikatsschlüssel erstellen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die gewünschte Datei, und navigieren Sie anschließend zu **File Encryption** > **Archivieren** > **Zertifikat**.
2. Wählen Sie einen **Zertifikatsspeicher**.
3. Klicken Sie auf **Zertifikate sammeln**.
4. Wählen Sie mindestens ein Zertifikat aus, und klicken Sie anschließend auf **OK**.

Hinweis

Zertifikate werden aus dem Windows Zertifikatsspeicher gesammelt.

5. Legen Sie einen leeren CD/DVD-Rohling in ein verfügbares optisches Laufwerk ein.
6. Wählen Sie das optische Laufwerk.
7. Klicken Sie auf **OK**.

Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

File Encryption – Archivieren und brennen

File Encryption Mit der Funktion **Archivieren und brennen** können Sie verschlüsselte Dateien auf eine CD oder DVD schreiben. Die Dateien sind selbstextrahierend und können mit einem festen Kennwort oder digitalen Zertifikat verschlüsselt werden.

Archiv mit einem festen Kennwort brennen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei, und navigieren Sie anschließend zu **File Encryption** > **Archivieren und brennen** > **Festes Kennwort**.
2. Geben Sie das Kennwort ein und bestätigen Sie es.
3. Legen Sie einen Rohling in das optische CD/DVD-Laufwerk.
4. Wählen Sie das optische Laufwerk.
5. Klicken Sie auf **OK**.

   Die selbstextrahierende Datei wird auf die CD/DVD gebrannt.

Archiv mit einem Zertifikat brennen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei, navigieren Sie anschließend zu **File Encryption** > **Archivieren und brennen** > **Zertifikat**.
2. Wählen Sie einen **Zertifikatsspeicher**.
3. Klicken Sie auf **Zertifikate sammeln**.
4. Wählen Sie mindestens ein Zertifikat aus, und klicken Sie anschließend auf **OK**.
5. Wählen Sie ein optisches Laufwerk aus, in dem eine leere CD/DVD eingelegt ist.

6. Klicken Sie auf **OK**.

   Die selbstextrahierende Datei wird auf die CD/DVD gebrannt.

File Encryption - Sicheres Löschen

Mit der Funktion "Sicheres Löschen" können Sie die ausgewählten Dateien und die Dateihistorie auf dem File Encryption Gerät sicher löschen.

Funktion "Sicheres Löschen" von File Encryption verwenden

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei, und navigieren Sie zu **File Encryption** > **Sicheres Löschen**.
2. Klicken Sie auf **Ja**, um die Datei dauerhaft zu löschen.

Kapitel 14

Full Disk Encryption

Mit Hilfe von obligatorischer starker Authentifizierung und Full Disk Encryption bietet Full Disk Encryption eine umfassende Endpunkt-Datensicherheit. Full Disk Encryption sichert nicht nur die Datendateien, sondern darüber hinaus alle Anwendungen, Registrierungseinstellungen, temporären Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Host-Betriebssystem, bis der Benutzer validiert wird.

Es werden folgende Themen behandelt:

- *Info über Full Disk Encryption auf Seite 14-2*
- *Endpoint Encryption Tools auf Seite 14-2*
- *Full Disk Encryption Preboot auf Seite 14-3*
- *Full Disk Encryption Konnektivität auf Seite 14-19*
- *Full Disk Encryption – Wiederherstellungskonsole auf Seite 14-21*
- *Full Disk Encryption Wiederherstellungsmethoden auf Seite 14-34*
- *Reparatur-CD auf Seite 14-37*
- *Patch-Verwaltung mit Full Disk Encryption auf Seite 14-45*

Info über Full Disk Encryption

Der Trend Micro Full Disk Encryption Agent kombiniert einen robusten AES256-Verschlüsselungsalgorithmus und obligatorische Authentifizierung, um Daten ohne Authentifizierung unzugänglich zu machen. Full Disk Encryption verhindert Datenverluste durch die Verschlüsselung des gesamten Laufwerks, einschließlich Betriebssystem-, Programm-, temporären und Endbenutzerdateien.

Full Disk Encryption kann flexibel eingesetzt werden und unterstützt je nach Bedarf Festplattenverschlüsselung auf Software- oder Hardwarebasis. Selbstverschlüsselnde Laufwerke vom Typ Seagate DriveTrust™, OPAL und OPAL2 werden unterstützt. Während Hardware-basierte Verschlüsselung leichter auf neuer Hardware bereitgestellt und verwaltet werden kann und eine höhere Leistungsstufe bietet, ist für die Software-basierte Verschlüsselung keine Hardware erforderlich und die Bereitstellung auf vorhandenen Endpunkten ist billiger.

Trend Micro PolicyServer steuert Richtlinien, die sich auf Full Disk Encryption auswirken. Auf diese Weise wird die komplette Endpunktsicherheit gewährleistet, die im gesamten Unternehmen zentral verwaltet wird. Full Disk Encryption ist netzwerkorientiert und aktualisiert Richtlinien, bevor die Authentifizierung zugelassen wird. Sie können Daten auf dem Endpunkt auch von einem entfernten Standort aus sperren oder löschen, bevor auf das Betriebssystem oder auf andere vertrauliche Daten zugegriffen wird.

Trend Micro Endpoint Encryption 5.0 Patch 1 erweitert den Funktionsbereich von Full Disk Encryption, indem eine Integration mit Verschlüsselungslösungen, die zum Host-Betriebssystem gehören, durch zwei neue Endpoint Encryption Agents möglich gemacht wird:

- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

Endpoint Encryption Tools

In der folgenden Tabelle werden die verschiedenen Tools beschrieben, die für Endpoint Encryption verfügbar sind.

TABELLE 14-1. Endpoint Encryption Tools

TOOL	BESCHREIBUNG
Wiederherstellungskonsole	Mit der Wiederherstellungskonsole führen Sie eine Datenwiederherstellung nach einem kritischen Betriebssystemfehler durch, analysieren und lösen Netzwerkprobleme und verwalten Benutzer und Protokolle.
Command Line Helper	Mit Command Line Helper erstellen Sie verschlüsselte Werte, um beim Erstellen von Installationsskripts die Anmeldedaten zu schützen.
Command Line Installer Helper	Mit Command Line Installer Helper generieren Sie Skripts für automatisierte Installationen und erstellen bei der Definition von Skripts verschlüsselte Werte für Anmeldedaten.
DAAutoLogin	Mit DAAutoLogin führen Sie Windows-Patches durch. Mit DAAutoLogin kann Endpoint Encryption Preboot einmalig umgangen werden.
Reparatur-CD	Mit der bootfähigen Reparatur-CD entschlüsseln Sie die Festplatte, bevor Sie Full Disk Encryption in Fällen entfernen, in denen der Datenträger beschädigt wurde. Die Reparatur-CD sollte nur dann verwendet werden, wenn die Standardmethoden zum Entfernen nicht durchführbar sind. Ein typisches Symptom einer beschädigten Festplatte ist ein schwarzer Bildschirm.

Full Disk Encryption Preboot

Nach der Installation von Full Disk Encryption wird jetzt Full Disk Encryption Preboot vor dem Laden von Windows angezeigt. Full Disk Encryption Preboot sorgt dafür, dass nur autorisierte Benutzer auf Endpunkte zugreifen können, und aktualisiert bei einer Verbindung mit PolicyServer die lokalen Sicherheitsrichtlinien.

Hinweis

Mit PolicyServer MMC können Sie wahlweise die Berücksichtigung der Groß- und Kleinschreibung von Benutzernamen aktivieren.

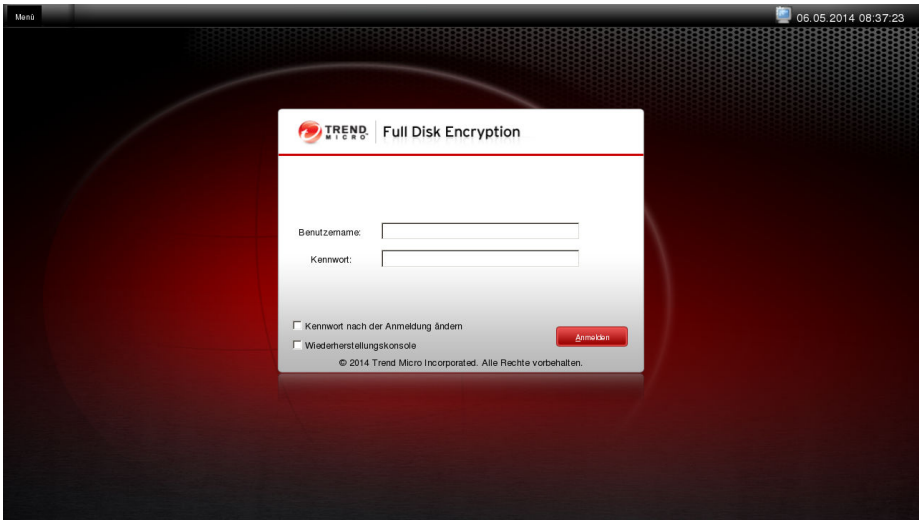


ABBILDUNG 14-1. DAS FULL DISK ENCRYPTION PREBOOT FENSTER

Menüoptionen

Im oberen linken Menü von Full Disk Encryption Preboot stehen mehrere Optionen zur Verfügung.

TABELLE 14-2. FULL DISK ENCRYPTION PREBOOT MENÜOPTIONEN

MENÜELEMENT	BESCHREIBUNG
Authentifizierung	Sie können die Authentifizierungsmethode wechseln, die zur Anmeldung bei Endpoint Encryption Geräten verwendet wird.
Kommunikation	Manuelle Synchronisierung mit PolicyServer. **Hinweis** Der Menübefehl **Kommunikation** ist für nicht verwaltete Endpunkte nicht verfügbar.

MENÜELEMENT	BESCHREIBUNG
Computer	Anzeige von Informationen über Full Disk Encryption, Ändern der Tastaturbelegung, Zugang zur Bildschirmtastatur oder Neustart bzw. Herunterfahren des Geräts.

Netzwerkverbindung

Das Symbol für die Netzwerkverbindung ( ) wird in der oberen rechten Ecke angezeigt, wenn Full Disk Encryption als verwalteter Endpunkt installiert ist. Dieses Symbol wird nur hervorgehoben, wenn das Gerät mit dem Netzwerk verbunden ist und eine Kommunikation mit dem PolicyServer stattfindet. Wenn Full Disk Encryption nicht verwaltet ist, wird das Netzwerksymbol nicht angezeigt.

Verbindung mit einem Wireless-Netzwerk aufbauen

Das Symbol für eine Wireless-Verbindung ( ) wird in der oberen rechten Ecke im Anmeldefenster von Full Disk Encryption Preboot angezeigt, wenn im Endpunkt eine WLAN-Netzwerkkarte installiert ist. Wenn keine WLAN-Netzwerkkarte erkannt wird, wird kein Wireless-Netzwerksymbol angezeigt.

Hinweis

Full Disk Encryption Preboot kann nicht automatisch die Authentifizierung für WEP-Sicherheit erkennen. Wenn es sich beim Authentifizierungstyp um WEP-OPEN oder WEP-PSK handelt, geben Sie den Sicherheitstyp manuell an.

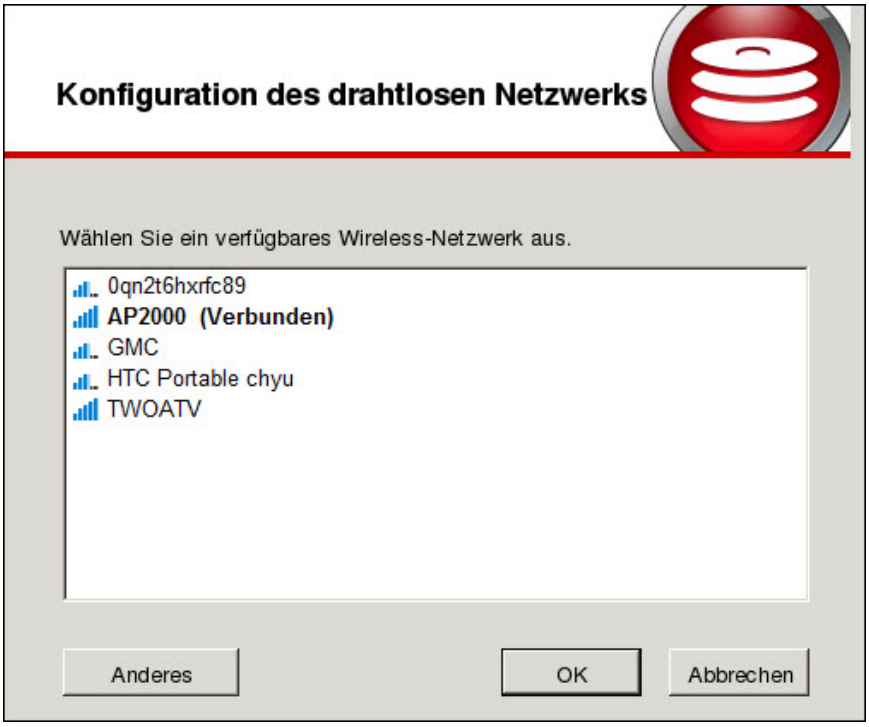
Prozedur

1. Klicken Sie auf das Wireless-Symbol in der oberen rechten Ecke des Anmeldefensters von Full Disk Encryption Preboot.

Das Fenster **Auf Verbindung zugreifen** wird angezeigt.

2. Klicken Sie auf **Alle Zugangspunkte**.

Das Fenster **Konfiguration des drahtlosen Netzwerks** wird angezeigt.



3. Wählen Sie eine der folgenden Optionen:

   - Um das aufgeführte Netzwerk zu verwenden, wählen Sie die SSID, und klicken Sie anschließend auf **OK**.
   - Um ein nicht aufgeführtes Netzwerk zu konfigurieren, klicken Sie auf **Anderes Netzwerk**, geben Sie die SSID-Einstellungen ein, und klicken Sie anschließend auf **Verbinden**.

4. Warten Sie, bis Full Disk Encryption den drahtlosen Zugang konfiguriert hat.

5. Klicken Sie auf **Schließen**, um die Einrichtung des Wireless-Netzwerks abzuschließen.

Bildschirmtastatur

Sie können von Full Disk Encryption Preboot auf die Bildschirmtastatur zugreifen. Navigieren Sie dazu zu **Menü** > **Computer** > **Bildschirmtastatur**.

Um den Cursor in das gewünschte Feld zu setzen, wenn die Tastatur angezeigt wird, klicken Sie in der unteren rechten Ecke der Tastatur auf **Fokus**.

Tastaturbelegung ändern

Wird die Tastaturbelegung geändert, so wirkt sich dies sowohl auf Tastatureingaben als auch auf die Bildschirmtastatur aus. Nach dem Starten von Windows wird die Tastaturbelegung vom Windows-Betriebssystem festgelegt. Ein Neustart ist erforderlich, um die Änderung der Tastaturbelegung zu übernehmen.

Prozedur

1. Navigieren Sie zu **Menü** > **Computer** > **Tastaturbelegung ändern**.

   Das Fenster **Wählen Sie die Sprache für das Tastaturlayout aus** wird angezeigt.

2. Wählen Sie ein Tastaturlayout aus.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf **OK**, um den Endpunkt neu zu starten.

Authentifizierungsmethode ändern

Hinweis

Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode auf Seite 2-7*.

Prozedur

1. Wählen Sie in Full Disk Encryption Preboot die Option **Kennwort nach der Anmeldung ändern**.

2. Geben Sie den Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt. Die Benutzeroberfläche unterscheidet sich je nach Authentifizierungsmethode.

ABBILDUNG 14-2. Beispiel zum Ändern eines festen Kennworts

4. Wählen Sie aus dem Menü oben links **Authentifizierung**, und wählen Sie dann die gewünschte Authentifizierungsmethode.

   Das Fenster **Neues Kennwort** der ausgewählten Authentifizierungsmethode wird angezeigt.

5. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Kennwörter ändern

Das folgende Verfahren erklärt, wie Sie das Kennwort für ein Endpoint Encryption Benutzerkonto mit Full Disk Encryption Preboot ändern.

Prozedur

1. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein.
2. Wählen Sie **Kennwort nach der Anmeldung ändern**.
3. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt. Die Benutzeroberfläche unterscheidet sich je nach Authentifizierungsmethode.

ABBILDUNG 14-3. Fenster zum Ändern eines festen Kennworts

4. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

ColorCode

ColorCode™ ist eine einzigartige Authentifizierungsmethode, bei deren Entwicklung eine schnelle Eingabe und eine leichte Merkfähigkeit im Vordergrund standen. Die ColorCode-Authentifizierung besteht nicht aus alphanumerischen Zeichen oder Symbolen, sondern aus einer vom Benutzer erstellten Farbfolge (Beispiel: rot, rot, blau, gelb, blau, grün).

ABBILDUNG 14-4. Das Fenster "ColorCode-Authentifizierung"

ColorCode-Kennwort erstellen

Die Gesamtanzahl von Schritten in ColorCode (Anzahl) wird von PolicyServer definiert. Die Standardanzahl ist 6.

Prozedur

1. Starten Sie den Endpunkt, und warten Sie, bis Full Disk Encryption Preboot angezeigt wird.
2. Folgen Sie den Anweisungen zum Ändern von Kennwörtern.

   Weitere Informationen finden Sie unter *Kennwörter ändern auf Seite 14-10*.
3. Ändern Sie die Authentifizierungsmethode in ColorCode.

Hinweis

Weitere Informationen über das Ändern von Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode ändern auf Seite 14-8*.

Das Fenster **ColorCode Kennwort ändern** wird angezeigt.

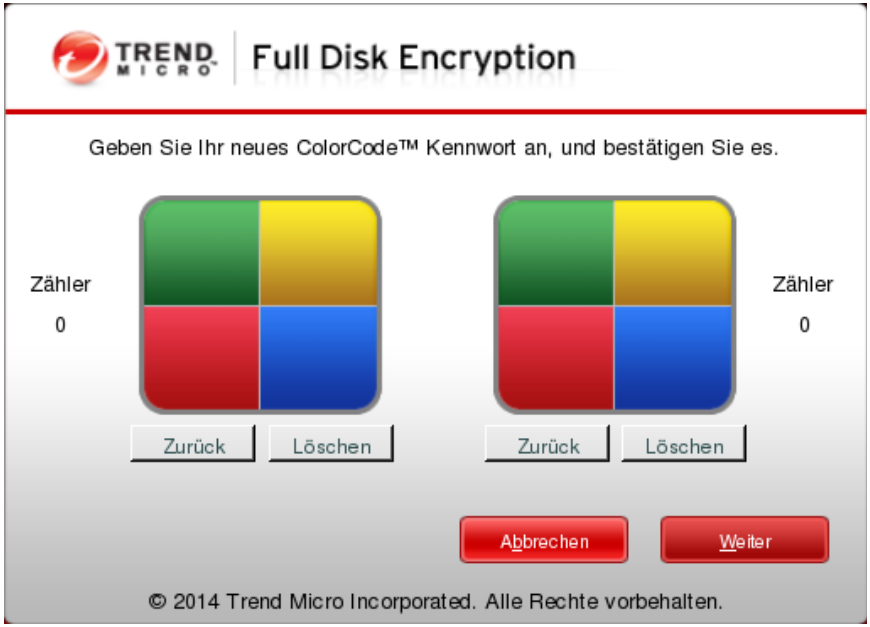


ABBILDUNG 14-5. Fenster "ColorCode Kennwort ändern"

4. Wählen Sie die erste Farbe, indem Sie im linken Quadrat darauf klicken.

   Die Anzahl erhöht sich um 1.

5. Klicken Sie auf die weiteren Farben in der Folge.

Tipp

Klicken Sie auf **Zurück**, um die zuletzt angeklickte Farbe zu ändern, oder klicken Sie auf **Löschen**, um von vorn zu beginnen.

6. Wenn der Vorgang abgeschlossen ist, bestätigen Sie das ColorCode-Kennwort im rechten Quadrat.

7. Klicken Sie zum Abschluss auf **Weiter**.

Remote-Hilfe

Mit der Remote-Hilfe können Gruppen- oder Unternehmensauthentifizierer ausgesperrte Endpoint Encryption Benutzer unterstützen, die sich nach zu vielen erfolglosen Versuchen oder, wenn zu viel Zeit seit der letzten PolicyServer Synchronisierung vergangen ist, nicht bei Endpoint Encryption Geräten anmelden können.

Remote-Hilfe zum Entsperren von Full Disk Encryption Geräten verwenden

Wichtig

- Durch einen Neustart des Endpoint Encryption Geräts wird der Herausforderungscode geändert.
- Durch eine manuelle Synchronisierung der Richtlinien mit PolicyServer wird der Herausforderungscode ebenfalls geändert.
- Bei Herausforderungscodes und Antwortcodes muss die Groß-/Kleinschreibung nicht berücksichtigt werden.

Prozedur

1. Navigieren Sie in Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Remote-Hilfe**.
2. Übermitteln Sie den **Herausforderungscode** an den Richtlinien-/Gruppenadministrator.
3. Geben Sie den **Antwortcode** ein, den Sie vom Richtlinien-/Gruppenadministrator erhalten haben.
4. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

   Hinweis

   Wenn für das Konto die Domänenauthentifizierung verwendet wird, startet der Endpunkt direkt in Windows.

5. Geben Sie das neue Kennwort an, bestätigen Sie es und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

SmartCard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch ein physisches Token zur Bestätigung der Identität des Benutzers. Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- Das Smartcard-Lesegerät ist mit dem Endpunkt verbunden, wobei sich die Smartcard im Lesegerät befindet.
- ActivClient 6.1 ist mit alle Service Packs und Updates installiert.
- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.

Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Hinweis

Smartcard-Authentifizierung kann nur mit PolicyServer MMC konfiguriert werden.

Aktivieren Sie die Smartcard-Authentifizierung für jeden Endpoint Encryption Agent:

- Navigieren Sie für File Encryption zu **Anmelden** > **Kennwort** > **Physischer Token erforderlich**.
- Navigieren Sie für Full Disk Encryption zu **Full Disk Encryption** > **Anmelden** > **Token-Authentifizierung**.

Smartcard-Registrierung

Smartcard-Zertifikate sind mit dem Benutzerkonto und der zugewiesenen Gruppe des Benutzer verbunden. Nach der Registrierung kann der Benutzer die Smartcard-Authentifizierung von jedem Endpoint Encryption Gerät in der betreffenden Gruppe verwenden. Benutzer können nach Belieben jedes Endpoint Encryption Gerät in ihrer Gruppe verwenden und müssen kein Einmalkennwort anfordern.

Registrieren Sie eine Smartcard, indem Sie eine der folgenden Methoden anwenden:

- Informationen zur Verwendung von Full Disk Encryption Preboot finden Sie unter *Eine Smartcard in Full Disk Encryption Preboot registrieren auf Seite 11-27*.
- Informationen zur Verwendung von PolicyServer MMC finden Sie unter *Smartcard-Authentifizierung in PolicyServer MMC konfigurieren auf Seite 11-25*.

Eine Smartcard in Full Disk Encryption Preboot registrieren

Prozedur

1. Folgen Sie den Anweisungen, um Kennwörter zu ändern, und wählen Sie anschließend **Smartcard**.

Weitere Informationen finden Sie unter *Benutzerkennwörter zurücksetzen auf Seite 11-23*.

2. Führen Sie die Smartcard in das Lesegerät ein.
3. Verbinden Sie das Lesegerät mit dem Endpunkt.
4. Geben Sie den Benutzernamen und das feste Kennwort ein.
5. Klicken Sie auf **Fortfahren**.
6. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **Fortfahren**.
7. Führen Sie im Fenster **Token registrieren** Folgendes aus:
   a. Geben Sie die neue PIN ein, die Sie vom Gruppen- oder Unternehmensadministrator erhalten haben.
   b. Bestätigen Sie die neue PIN.
   c. Wählen Sie den Typ der Smartcard aus dem Listenfeld **Token** aus.
   d. Klicken Sie auf **Fortfahren**, um die Registrierung des Smartcard-Tokens abzuschließen.

Selbsthilfe

Mit der Selbsthilfe-Authentifizierung können Endpoint Encryption Benutzer, die ihre Anmeldedaten vergessen haben, ohne die Hilfe durch den technischen Support Sicherheitsfragen beantworten und sich bei Endpoint Encryption Geräten anmelden. Die Selbsthilfe ist für Unternehmens- oder Gruppenadministrator- und Authentifiziererkonten nicht verfügbar. Die Selbsthilfe macht es erforderlich, dass Endpoint Encryption Benutzer auf die persönlichen Fragen der Selbsthilfe mit ihren vordefinierten persönlichen Antworten reagieren. Mit der Selbsthilfe kann ein festes Kennwort oder eine andere Authentifizierungsmethode ersetzt werden.

Hinweis

Die Selbsthilfe kann nur mit PolicyServer MMC konfiguriert werden.

Vergewissern Sie sich, dass die Selbsthilfe-Authentifizierung zugelassen wird. Weitere Informationen finden Sie unter *Authentifizierungsrichtlinien auf Seite 9-34*.

Warnung!

Die Selbsthilfe kann aus maximal sechs Fragen bestehen. Erstellen Sie nicht mehr als sechs Fragen, sonst können sich die Benutzer nicht mit der Selbsthilfe-Authentifizierung anmelden.

Selbsthilfe einrichten

Wenn die Selbsthilfe-Richtlinie aktiviert ist, wird der Benutzer nach der ersten Anmeldung aufgefordert, Antworten auf diese Selbsthilfe-Fragen festzulegen. Wenn Benutzer ihr Kennwort ändern, müssen sie die Selbsthilfe-Fragen erneut festlegen.

Hinweis

Die Antworten zur Selbsthilfe werden auf dem Gerät gespeichert. Wenn ein Benutzer sich bei einem anderen Full Disk Encryption Gerät anmeldet, muss er Antworten für die Selbsthilfe für dieses Gerät festlegen.

Prozedur

1. Geben Sie den Benutzernamen und das Kennwort ein.
2. Klicken Sie auf **Anmelden**.

   Das Fenster **Selbsthilfe** wird angezeigt.
3. Legen Sie Antworten auf alle Selbsthilfe-Fragen fest.
4. Klicken Sie auf **Weiter**.

   Das Gerät startet Windows.

Selbsthilfe verwenden

Prozedur

1. Wechseln Sie im oberen linken Menü von Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Selbsthilfe**.

   Das Fenster **Selbsthilfe** wird angezeigt.

2. Beantworten Sie alle Fragen zur Selbsthilfe.

3. Klicken Sie auf **Anmelden**.

4. Legen Sie ein neues Kennwort fest und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Antworten für die Selbsthilfe ändern

Prozedur

1. Geben Sie in Full Disk Encryption Preboot Ihre Anmeldedaten ein, wählen Sie **Kennwort nach der Anmeldung ändern**, und klicken Sie anschließend auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

2. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Fenster **Selbsthilfe** wird angezeigt.

3. Legen Sie neue Antworten auf alle Selbsthilfe-Fragen fest, und klicken Sie anschließend auf **Weiter**.

   Auf dem Endpoint Encryption Gerät wird Windows gestartet.

Full Disk Encryption Konnektivität

Endpoint Encryption verwendet einen zugelassenen FIPS 140-2-Verschlüsselungsprozess für Daten, die zwischen Full Disk Encryption Preboot und PolicyServer übertragen werden. Full Disk Encryption Agents haben eine Netzwerkverbindung zum PolicyServer und können Richtlinien-Updates empfangen und Audit-Daten vom Agent hochladen. Die gesamte Client-Server-Kommunikation wird intern verschlüsselt und kann über ungesicherte Verbindungen wie das Internet gesendet werden.

Sie können den PolicyServer innerhalb einer DMZ (Demilitarisierte Zone) platzieren, um ihn sowohl für interne Netzwerke als auch das Internet zugänglich zu machen. Informationen zu verschiedenen Konfiguration der Netzwerktopologie finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

TABELLE 14-3. Full Disk Encryption Konnektivitätsanforderungen

RESSOURCE	FUNKTION
PolicyServer	Aktualisierte Sicherheitsrichtlinien vom PolicyServer können an Full Disk Encryption Preboot oder mit Hilfe von Verbindungen innerhalb von Windows, LAN oder VPN gesendet werden.
TCP/IP-Zugriff	Netzwerkverbindungen erfordern vollen TCP/IP-Netzwerkzugriff. DFÜ- oder Telefonzugriff kann nicht zur Bereitstellung der Verbindung mit dem PolicyServer während der Preboot-Authentifizierung verwendet werden.
Port	Endpoint Encryption Agents verwenden für die Kommunikation standardmäßig Port 8080. Um die Standardportnummer zu ändern, navigieren Sie zur Wiederherstellungskonsole und aktualisieren Sie den PolicyServer. Weitere Informationen finden Sie unter *Full Disk Encryption PolicyServer wechseln auf Seite 14-24*.

Automatische Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Endpoint Encryption Agents und PolicyServer einleiten.

- Nachdem das Betriebssystem geladen wird und der Dienst des Endpoint Encryption Agent startet

  Hinweis

  Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- Wenn Full Disk Encryption Preboot startet (nur Full Disk Encryption)
- Die Zeitdauer der Richtlinie **Synchronisierungsintervall** läuft ab

Öffnen Sie das Fenster **Info über**, um Endpoint Encryption Agent anzuweisen, die Richtlinien manuell zu synchronisieren.

Hinweis

Aktionen für Endpoint Encryption Geräte werden eingeleitet, nachdem der Endpoint Encryption Agent Richtlinien-Updates erhält.

Aktualisieren von Full Disk Encryption Agents

Full Disk Encryption Agents erhalten automatisch Sicherheitsrichtlinien-Updates vom PolicyServer in Intervallen, die von der Richtlinie vorgegeben werden.

Führen Sie eine der folgenden Aktionen aus, um Richtlinien manuell zu aktualisieren.

Prozedur

- Verwenden Sie Full Disk Encryption Preboot.

  a. Navigieren Sie zu **Kommunikation** > **Richtlinien synchronisieren**.

  b. Navigieren Sie zu **Computer** > **Info über Full Disk Encryption**.

Der Zeitstempel der aktuellsten PolicyServer Richtliniensynchronisierung wird angezeigt.

- Verwenden Sie den Full Disk Encryption Agent.

  a. Doppelklicken Sie in der Windows-Task-Leiste auf das Full Disk Encryption-Symbol ( ).

     Der Full Disk Encryption Agent wird geöffnet.

  b. Klicken Sie auf **Mit PolicyServer synchronisieren**.

     Nach kurzer Zeit setzt PolicyServer alle neue Richtlinienänderungen durch.

Full Disk Encryption – Wiederherstellungskonsole

Die Wiederherstellungskonsole unterstützt Sie dabei, Full Disk Encryption Geräte wiederherzustellen, wenn es zu einem Ausfall des primären Betriebssystems kommt, Sie nach Lösungen für Probleme mit der Netzwerkverbindung suchen und Richtlinien verwalten, jedoch nicht mit PolicyServer verbunden sind.

Warnung!

Verwenden Sie die Wiederherstellungskonsole vor dem Ausführen der Standard-Diagnose- und Reparaturprogramme von Windows.

Alle Änderungen an Richtlinien werden überschrieben, wenn der Full Disk Encryption Agent Richtlinien mit PolicyServer synchronisiert.

Optionen der Wiederherstellungskonsole

KONSOLENMENÜ	BESCHREIBUNG
Zurück zur Anmeldung	Beendet die Wiederherstellungskonsole und kehrt zum Anmeldefenster zurück.

KONSOLENMENÜ	BESCHREIBUNG
Festpl. entschlüss.	Verschlüsselung von der Festplatte entfernen. Verwenden Sie die Full Disk Encryption Preboot-Wiederherstellungskonsole, um auf die Option "Festplatte entschlüsseln" zuzugreifen.
Partit. bereitst.	Bereitstellung von Zugriff auf die verschlüsselten Partitionen zur Dateiverwaltung. Verwenden Sie die Full Disk Encryption Preboot-Wiederherstellungskonsole, um auf die Option "Partitionen bereitstellen" zuzugreifen. **Hinweis** Auf "Partitionen bereitstellen" kann nur von Geräten mit Softwareverschlüsselung aus zugegriffen werden. Diese Option ist abgeblendet, wenn ein Gerät über Hardware-Verschlüsselung verfügt.
Boot wiederherst.	Rollback des MBR zu einem Zustand vor der Installation von Full Disk Encryption. Verwenden Sie die Full Disk Encryption Preboot-Wiederherstellungskonsole, um auf die Option "Bootsektor wiederherstellen" zuzugreifen. **Hinweis** Auf "Bootsektor wiederherstellen" kann nur von Geräten mit Softwareverschlüsselung aus zugegriffen werden. Diese Option ist abgeblendet, wenn ein Gerät über Hardware-Verschlüsselung verfügt.
Benutzer verwalten	Hinzufügen oder Entfernen von Benutzern von einem Gerät, wenn es nicht mit dem PolicyServer verbunden ist.
Richtlinien verwalten	Ändern Sie die Richtlinien für Geräte, die entweder nicht von PolicyServer verwaltet werden oder die verwaltet werden, aber die vorübergehend nicht mit PolicyServer verbunden sind. Wenn das Gerät verwaltet ist, werden Richtlinienänderungen bei der nächsten Kommunikation des Geräts mit PolicyServer überschrieben.

KONSOLENMENÜ	BESCHREIBUNG
Protokolle anzeigen	Anzeigen und Durchsuchen verschiedener Full Disk Encryption Protokolle. **Hinweis** Protokolle sind nur verfügbar, wenn von Windows aus auf die Wiederherstellungskonsole zugegriffen wird.
Netzwerk-Setup	Überprüfen, Testen und Ändern von Netzwerkeinstellungen.
Beenden	Beenden der Wiederherstellungskonsole.

Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen

Nur Unternehmens- oder Gruppenadministrator- und -authentifiziererkonten können auf die Wiederherstellungskonsole zugreifen.

Prozedur

1. Aktivieren Sie die folgende Richtlinie, um Benutzern zu erlauben, auf die Wiederherstellungskonsole zuzugreifen:

   Full Disk Encryption > **Agent** > **Wiederherstellung durch Benutzer zulassen**

2. Starten Sie den Endpunkt neu.

   Full Disk Encryption Preboot wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Wiederherstellungskonsole**.

4. Geben Sie die Anmeldedaten für das Endpoint Encryption Benutzerkonto ein.

5. Klicken Sie auf **Anmelden**.

   Die Wiederherstellungskonsole wird geöffnet.

Auf die Wiederherstellungskonsole von Windows aus zugreifen

Prozedur

1. Wechseln Sie unter Windows zum Installationsverzeichnis von Full Disk Encryption.

   Der Standardordner ist `C:\Program Files\Trend Micro\Full Disk Encryption\`.

2. Öffnen Sie `RecoveryConsole.exe`.

   Das Fenster **Wiederherstellungskonsole** wird angezeigt.

3. Geben Sie den Endpoint Encryption Benutzernamen und das Kennwort ein, und klicken Sie anschließend auf **Anmelden**.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatte entschlüsseln** geöffnet.

PolicyServer Einstellungen für Full Disk Encryption

Sie können die PolicyServer Einstellungen für Full Disk Encryption konfigurieren, indem Sie von Full Disk Encryption Preboot aus die Wiederherstellungskonsole öffnen oder indem Sie die Datei `C:\Program Files\Trend Micro\Full Disk Encryption\RecoveryConsole.exe` ausführen.

Full Disk Encryption PolicyServer wechseln

Hinweis

Ein Wechsel des PolicyServer erfordert Zugriff auf die Full Disk Encryption Wiederherstellungskonsole. Weitere Informationen finden Sie unter *PolicyServer Einstellungen für Full Disk Encryption auf Seite 14-24*.

Prozedur

1. Klicken Sie auf der Full Disk Encryption Wiederherstellungskonsole auf die Registerkarte **PolicyServer**.
2. Klicken Sie auf **Server wechseln**.
3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
4. Geben Sie die neue Serveradresse ein.
5. Klicken Sie auf **Speichern**.

"Festplatte entschlüsseln" verwenden

Durch Auswählen von **Festplatte entschlüsseln** wird eine verschlüsselte Full Disk Encryption Festplatte entschlüsselt, aber die Treiber für die Verschlüsselung werden nicht entfernt. Wenn Sie **Festplatte entschlüsseln** verwenden, deaktivieren Sie den Full Disk Encryption Dienst „DrAService“, bevor Sie Windows starten.

Warnung!

Lesen Sie die Anweisungen zu diesem Verfahren, bevor Sie **Festplatte entschlüsseln** verwenden. Bei falscher Vorgehensweise kann der Verlust von Daten nicht ausgeschlossen werden. Entfernen Sie Full Disk Encryption nicht mit Hilfe von **Festplatte entschlüsseln**, wenn das Endpoint Encryption Gerät normal funktioniert. Verwenden Sie stattdessen `TMFDEUninstall.exe`.

Prozedur

1. Melden Sie sich an der Wiederherstellungskonsole an.

   Weitere Informationen finden Sie unter *Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen auf Seite 14-23*.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatte entschlüsseln** geöffnet.

2. Klicken Sie auf **Entschlüsseln**, um mit der Entschlüsselung des Laufwerks zu beginnen.

Mit der Entschlüsselung wird direkt begonnen, und es wird die Seite **Festplatte entschlüsseln** mit dem Entschlüsselungsfortschritt angezeigt.

3. Klicken Sie nach Beendigung der Entschlüsselung auf **Beenden**, um das Endpoint Encryption Gerät neu zu starten.

4. Wählen Sie eine der folgenden Optionen:

   - Beim Starten mit einer CD, DVD oder einem USB-Dongle mit einem Reparaturtool:

     a. Nach der Beendigung von Full Disk Encryption drücken Sie **F12** (oder die entsprechende Taste, um zu den Boot-Optionen zu gelangen).

     b. Legen Sie die Reparatur-CD ein, und wählen Sie im Fenster mit den Boot-Optionen "CD/DVD-Laufwerk".

     c. Fahren Sie mit den etablierten Wiederherstellungsmaßnahmen fort.

   - Beim Starten von Windows:

     a. Starten Sie den Endpunkt neu, und halten Sie **F8** gedrückt.

     b. Wählen Sie **Abgesicherter Modus**, bevor das System beginnt, Windows zu starten.

Warnung!

Wenn Sie das Fenster mit den Windows Boot-Optionen verpassen, schalten Sie das Gerät sofort aus. Wenn Windows normal gestartet wird (nicht im abgesicherten Modus), wird DrAService sofort damit beginnen, die Festplatte erneut zu verschlüsseln. Bei allen Wiederherstellungsmaßnahmen, die an diesem Punkt durchgeführt werden, besteht das Risiko, dass die Daten auf der Festplatte irreparabel beschädigt werden.

---

5. Öffnen Sie **Geräteverwaltung**, und navigieren Sie zu **Dienste und Anwendungen** > **Dienste**.

   Das Fenster **Dienste** wird angezeigt.

6. Blättern Sie zu **Trend Micro Full Disk Encryption**, und doppelklicken Sie darauf, um das Fenster **Eigenschaften von Trend Micro Full Disk Encryption** zu öffnen.

7. Ändern Sie auf der Registerkarte **Allgemein** den **Starttyp** in **Deaktiviert**.
8. Klicken Sie auf **Übernehmen**, und klicken Sie anschließend auf **OK**.
9. Starten Sie den Endpunkt neu.
10. Melden Sie sich bei Full Disk Encryption Preboot an.
11. Melden Sie sich bei Windows an.
12. Nach dem Abschluss aller Wiederherstellungsaktionen legen Sie für **DrAService** den Starttyp **Automatisch** fest. Das Geräte verschlüsselt die Festplatte nach dem nächsten Neustart automatisch erneut.

Partit. bereitst.

Kopieren Sie mit Hilfe von **Partitionen bereitstellen** Dateien zwischen der verschlüsselten externen Festplatte und einem Speichergerät, bevor Sie ein Image der Festplatte erstellen oder diese neu formatieren. Der verschlüsselte Inhalt auf dem Laufwerk wird im linken Fensterbereich angezeigt, und das unverschlüsselte Gerät kann im rechten Fensterbereich gemountet werden. Verschieben Sie Dateien mit Kopieren und Einfügen zwischen den Fensterbereichen. Dateien, die auf das verschlüsselte Laufwerk kopiert werden, werden verschlüsselt. Bei Dateien, die vom verschlüsselten Laufwerk kopiert werden, wird die Verschlüsselung aufgehoben.

Boot wiederherst.

Mit Hilfe der Option **Bootsektor wiederherstellen** wird der ursprüngliche Bootsektor des Endpoint Encryption Geräts wiederhergestellt, wenn das Gerät vollständig entschlüsselt ist. **Bootsektor wiederherstellen** ist nur über Full Disk Encryption Preboot verfügbar.

Entschlüsseln Sie die Festplatte, bevor Sie den Master Boot Record (MBR) wiederherstellen.

Warnung!

Sie sollten jedoch **Festplatte entschlüsseln** nicht aufrufen, bevor Sie die Anweisungen gelesen haben. Datenverluste können auftreten.

Prozedur

1. Melden Sie sich an der Wiederherstellungskonsole an.

   Weitere Informationen finden Sie unter *Von Full Disk Encryption Preboot auf die Wiederherstellungskonsole zugreifen auf Seite 14-23*.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatte entschlüsseln** geöffnet.

2. Klicken Sie auf **Festplatte entschlüsseln**, und klicken Sie anschließend auf **Entschlüsseln**.

3. Wechseln Sie zur Option **Bootsektor wiederherstellen**.

   Das Bestätigungsfenster **Möchten Sie den MBR wirklich ersetzen?** wird angezeigt.

4. Klicken Sie auf **Ja**, um den MBR zu ersetzen.

   Eine Nachricht mit der Bestätigung, dass der MBR ersetzt wurde, wird angezeigt.

5. Klicken Sie auf **Beenden**.

   Auf dem Endpoint Encryption Gerät wird Windows gestartet.

Full Disk Encryption Benutzer verwalten

Bei der Verwaltung von Benutzern mit **Benutzer verwalten** werden Benutzer dem Full Disk Encryption Preboot-Cache hinzugefügt bzw. daraus entfernt, oder das im Cache gespeicherte Kennwort des Benutzers wird geändert. Die Option **Benutzer verwalten** ist nützlich, wenn der Full Disk Encryption Agent keine Verbindung zum PolicyServer aufbauen kann. Diese Option kann sowohl von Full Disk Encryption Preboot als auch von der Windows Wiederherstellungskonsole verwendet werden.

Hinweis

- **Benutzer verwalten** ist nur verfügbar, wenn keine Verbindung mit PolicyServer besteht.
- Änderungen, die an Benutzern vorgenommen wurden, werden überschrieben, wenn Full Disk Encryption eine Verbindung zu PolicyServer aufbaut.

Einige Überlegungen zu Kennwörtern:

- Bei zugewiesenen Kennwörtern handelt es sich immer um feste Kennwörter.
- Legen Sie das Ablaufdatum für das Benutzerkennwort mit Hilfe des Kalenders **Kennwort läuft ab** fest.
- Wenn Sie als Datum das aktuelle Datum oder ein älteres Datum festlegen, wird eine sofortige Kennwortänderung durchgesetzt. Wenn Sie als Datum ein zukünftiges Datum festlegen, wird die Änderung an dem angegebenen Datum umgesetzt.

Benutzer bearbeiten

Die Bearbeitung von Benutzern in der Wiederherstellungskonsole folgt denselben Regeln, die auch für das Unternehmen gelten. Weitere Informationen zu Rollen und Authentifizierung finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*.

Prozedur

1. Wählen Sie den Benutzer aus der Benutzerliste aus.
2. Aktualisieren Sie die gewünschten Informationen.
3. Wählen Sie den Benutzertyp.

   Eine Erklärung der Kontorollen finden Sie unter *Übersicht über Geräte und Benutzer auf Seite 2-1*.
4. Legen Sie das Ablaufdatum für das Kennwort fest.
5. Klicken Sie auf **Speichern**.

Das Benutzerkonto wird aktualisiert.

Benutzer hinzufügen

Prozedur

1. Klicken Sie auf **Benutzer hinzufügen**.
2. Geben Sie Ihren Benutzernamen und das Kennwort ein, und bestätigen Sie dann das Kennwort.
3. Wählen Sie die Authentifizierungsmethode aus der Dropdown-Liste **Authentifizierungstyp**.
4. Legen Sie das Ablaufdatum für das Kennwort fest.
5. Klicken Sie auf **Speichern**.

   Der neue Benutzer wird in der Benutzerliste angezeigt, und ein Bestätigungsfenster erscheint.
6. Klicken Sie auf **OK**, um das Bestätigungsfenster zu schließen.

   Das neue Benutzerkonto wird hinzugefügt.

Benutzer löschen

Prozedur

1. Wählen Sie einen Benutzer aus der Benutzerliste aus.
2. Klicken Sie auf **Benutzer löschen**.

   Ein Bestätigungsfenster zum Löschen des Benutzers wird angezeigt.
3. Klicken Sie auf **Ja**.

   Der Benutzer wird aus der Benutzerliste gelöscht.

Richtlinien verwalten

Verwenden Sie **Richtlinien verwalten**, um die verschiedenen Richtlinien für die Full Disk Encryption Wiederherstellungskonsole festzulegen. Eine Erklärung dieser Richtlinien finden Sie unter *Richtlinien in PolicyServer MMC auf Seite 9-1*.

Hinweis

Die Option **Richtlinien verwalten** ist nur verfügbar, wenn keine Verbindung mit PolicyServer besteht. Die vorgenommenen Änderungen werden überschrieben, wenn Full Disk Encryption das nächste Mal eine Verbindung zu PolicyServer aufbaut.

Protokolle anzeigen

Wählen Sie **Protokolle anzeigen**, um auf Grundlage bestimmter Kriterien nach Protokollen zu suchen und diese anzuzeigen. **Protokolle anzeigen** ist nur in der Wiederherstellungskonsole unter Windows verfügbar. Der Befehl ist über Full Disk Encryption Preboot nicht verfügbar.

Informationen über das Anzeigen von Full Disk Encryption Protokollen finden Sie unter *Auf die Wiederherstellungskonsole von Windows aus zugreifen auf Seite 14-24*.

Netzwerk-Setup

Das Netzwerk-Setup wird zum Überprüfen, Testen und/oder Ändern der Netzwerkeinstellungen von Full Disk Encryption Preboot verwendet. Es stehen drei Registerkarten zur Verfügung: **IPv4**, **IPv6** und **PolicyServer**.

Netzwerkkonfiguration verwalten

Standardmäßig ist **Einstellungen von Windows abrufen** für IPv4 und IPv6 ausgewählt. Deaktivieren Sie diese Option, um die Netzwerkeinstellungen manuell zu konfigurieren.

- Die Auswahl von **DHCP** (IPv4) oder **Adresse automatisch abrufen** (IPv6) verwendet die dynamisch zugewiesene IP-Adresse.

- Bei Auswahl von **Statische IP-Adresse** werden alle Felder in diesem Abschnitt aktiviert.
- Wenn Sie auf der Registerkarte **IPv6** die Option **Statische IP-Adresse** auswählen und das Feld "IP-Adresse" leer ist, wird eine eindeutige IP-Adresse auf Grundlage der Hardware-Adresse des Computers erzeugt.

Full Disk Encryption in ein anderes Unternehmen migrieren

Eine PolicyServer Instanz kann mehrere Unternehmenskonfigurationen haben, die einen Geschäftsbereich oder eine Abteilung repräsentieren. Wenn Sie ein Gerät in ein neues Unternehmen verschieben, wird das Endpoint Encryption Gerät aus dem alten Unternehmen entfernt und dem neuen Unternehmen innerhalb derselben PolicyServer Instanz hinzugefügt. Möglicherweise muss der Full Disk Encryption Agent in ein neues Unternehmen verschoben werden, wenn der Mitarbeiter in eine andere Abteilung oder an einen anderen Standort versetzt wird.

Hinweis

Informationen über das Wechseln des PolicyServer, der den Full Disk Encryption Agent verwaltet, finden Sie unter *Full Disk Encryption PolicyServer wechseln auf Seite 14-24*.

Ein Wechsel des Unternehmens erfordert Zugriff auf die Full Disk Encryption Wiederherstellungskonsole. Weitere Informationen finden Sie unter *PolicyServer Einstellungen für Full Disk Encryption auf Seite 14-24*.

Warnung!

Wenn Sie das Unternehmen wechseln, müssen Sie die Richtlinien erneut konfigurieren und die Gruppen neu erstellen. Die gespeicherten Kennwörter, der Kennwortverlauf und die Audit-Protokolle werden gelöscht.

Prozedur

1. Klicken Sie auf **Netzwerk-Setup**.
2. Wählen Sie die Registerkarte **PolicyServer**.
3. Klicken Sie auf **Unternehmen wechseln**.

Das Fenster **Unternehmen wechseln** wird angezeigt.

ABBILDUNG 14-6. WIEDERHERSTELLUNGSKONSOLE – UNTERNEHMEN WECHSELN

4. Konfigurieren Sie die folgenden Optionen:

OPTION	BEZEICHNUNG
Neuer Serverbenutzer	Geben Sie den Kontonamen eines Unternehmensadministrators oder den Benutzernamen eines Kontos an, das berechtigt ist, Installationen im Unternehmen oder der Gruppe im neuen PolicyServer durchzuführen.
Neues Benutzerkennwort	Geben Sie das Kennwort für den Unternehmensadministrator an.
Neue Serveradresse	Geben Sie die neue IP-Adresse oder den neuen Host-Namen für den PolicyServer ein.

Option	Bezeichnung
Neues Unternehmen	Geben Sie das neue Unternehmen für den PolicyServer an.

5. Klicken Sie auf **Speichern**.

   Full Disk Encryption validiert die neuen Informationen für den PolicyServer.

6. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Full Disk Encryption PolicyServer wechseln

Hinweis

Ein Wechsel des PolicyServer erfordert Zugriff auf die Full Disk Encryption Wiederherstellungskonsole. Weitere Informationen finden Sie unter *PolicyServer Einstellungen für Full Disk Encryption auf Seite 14-24*.

Prozedur

1. Klicken Sie auf der Full Disk Encryption Wiederherstellungskonsole auf die Registerkarte **PolicyServer**.
2. Klicken Sie auf **Server wechseln**.
3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
4. Geben Sie die neue Serveradresse ein.
5. Klicken Sie auf **Speichern**.

Full Disk Encryption Wiederherstellungsmethoden

Sobald das Full Disk Encryption Gerät vollständig verschlüsselt ist, sind Szenarien möglich, in denen Sie Aktionen für eine Systemwiederherstellung durchführen müssen,

beispielsweise ein vergessenes Kennwort des lokalen Administrators oder eine beschädigte Windows-Umgebung.

Wichtig

Entschlüsseln Sie das Laufwerk, bevor Sie Funktionen zur Wiederherstellung durchführen. Bei einer Software-Verschlüsselung können herkömmliche Tools zur Datenwiederherstellung (Windows Recovery Disk, ERD Commander, UBCD) nicht auf ein mit Full Disk Encryption 5.0 Patch 1 oder höher verschlüsseltes Laufwerk zugreifen.

Methoden zur Datenwiederherstellung stehen den Administrator- und Authentifiziererkonten für Endpoint Encryption zur Wiederherstellung von Daten zur Verfügung, wenn das Full Disk Encryption Gerät nicht ordnungsgemäß funktioniert.

Hinweis

Damit das Full Disk Encryption Laufwerk entschlüsselt werden kann, muss es sich beim Benutzer um einen Endpoint Encryption Unternehmens- oder Gruppenadministrator handeln. Damit alle Benutzer in einer Gruppe/Richtlinie Zugriff auf die Wiederherstellungskonsole haben, aktivieren Sie die folgende Richtlinie:

MANAGEMENT-KONSOLE	MENÜPFAD
PolicyServer MMC	Navigieren Sie zu **Full Disk Encryption** > **Agent** > **Wiederherstellung durch Benutzer zulassen**.
Control Manager	Erstellen oder bearbeiten Sie eine Richtlinie, navigieren Sie anschließend zu **Full Disk Encryption** > **Benutzer sind berechtigt, auf die Systemwiederherstellungstools zuzugreifen**.

Wiederherstellungsfunktionen für Full Disk Encryption-geschützte Geräte

Wiederherstellungsmethode	Beschreibung	Timing der Nutzung
Deinstallation von Full Disk Encryption	Bei der Deinstallation von Full Disk Encryption wird Full Disk Encryption vom Gerät entfernt. Nachdem die Deinstallation abgeschlossen ist, können Sie unter Windows mit etablierten Wiederherstellungsmaßnahmen fortfahren.	Windows-Umgebung arbeitet normal.
Wiederherstellungskonsole	Bei Auswahl der Full Disk Encryption Option **Wiederherstellungskonsole** > **Festplatte entschlüsseln** wird die ausgewählte Festplatte direkt entschlüsselt oder das Image der entschlüsselten Festplatte auf einem Wechseldatenträger gespeichert. **Hinweis** Diese Methode sollte nicht ausgeführt werden, wenn Windows normal funktioniert.	Full Disk Encryption Preboot wird geladen, Windows jedoch nicht.

Wiederherstellungsmethode	Beschreibung	Timing der Nutzung
Reparatur-CD	Eine bootfähige CD zum Entschlüsseln eines beschädigten Laufwerks, wenn das Gerät nicht von Full Disk Encryption Preboot gestartet werden kann. Ein typisches Symptom einer beschädigten Festplatte ist ein schwarzer Bildschirm. **Warnung!** Nicht verwenden, wenn Windows normal funktioniert.	• Full Disk Encryption Preboot wird nicht geladen. • Full Disk Encryption kann nicht authentifiziert werden.

Reparatur-CD

Bei der Full Disk Encryption Reparatur-CD handelt es sich um eine bootfähige CD, mit deren Hilfe ein Gerät vollständig entschlüsselt werden kann, wenn das Gerät nicht mehr in der Lage ist, gestartet zu werden.

Hinweis

- Bei einer physischen Beschädigung der Festplatte lässt sich das Laufwerk möglicherweise nicht vollständig entschlüsseln und könnte unbrauchbar sein.
- Wenn sich auf der Festplatte fehlerhafte Sektoren befinden, versucht Endpoint Encryption, die fehlerhaften Sektoren während der Entschlüsselung zu überspringen. Je nach Menge der fehlerhaften Sektoren wird dadurch die Leistung verringert. Wenn sich die fehlerhaften Sektoren an kritischen Positionen befinden, ist die Festplatte möglicherweise unbrauchbar.
- Vergewissern Sie sich vor dem Booten von der Reparatur-CD, dass das Festplattenkabel ordnungsgemäß angeschlossen ist.

Optionen der Reparatur-CD

In der folgenden Tabelle werden die auf der Full Disk Encryption Reparatur-CD verfügbaren Optionen beschrieben. Die Tabellen sollen Ihnen ein Verständnis über die richtige Verwendung der Funktionen vermitteln, die nach dem Booten mit der Full Disk Encryption Reparatur-CD verfügbar sind.

Grundlegende Optionen der Reparatur-CD

OPTIONEN	BESCHREIBUNG
Wiederherstellungskonsole	Startet die Wiederherstellungskonsole.
Gerät entsperren	Entsperrt ein Gerät, das aus folgenden Gründen gesperrt wurde: • Es sind viele erfolglose Anmeldeversuche erfolgt. • Keine Kommunikation mit PolicyServer für eine bestimmte Dauer **Hinweis** Die Option zum Entsperren ist nur verfügbar, wenn die Richtlinien-Remote-Authentifizierung auf **Abmelden** festgelegt ist.
Computer neu starten	Startet das Gerät neu.
Erweiterte Optionen	Bietet Zugriff auf erweiterte Optionen: • Full Disk Encryption Preboot entfernen • Löschen • Entschlüsselung erzwingen

Erweiterte Optionen der Reparatur-CD

Erweiterte Option	Beschreibung
Preboot entfernen	Entfernt das Full Disk Encryption Preboot Authentifizierungsfenster vom Gerät. **Warnung!** Diese Aktion kann nicht rückgängig gemacht werden. Dabei wird das Laufwerk nicht entschlüsselt. Entfernen Sie die Verschlüsselung mit der Option "Festplatte entschlüsseln".
Festplatte löschen	Entfernt alle Daten vom Gerät.
Entschlüsselung erzwingen	Entschlüsselt das Laufwerk, wenn Full Disk Encryption nicht gestartet werden kann.
Zurück zum Hauptmenü	Kehrt zu den Standard-CD-Optionen zurück.

Warnung!

Bei falscher Anwendung der **erweiterten Optionen** besteht das Risiko von Datenverlusten.

Daten mit der Reparatur-CD wiederherstellen

Mit der Reparatur-CD können Sie versuchen, Daten von einem verschlüsselten Laufwerk wiederherzustellen. Es gibt jedoch mehrere Überlegungen, die Sie beachten sollten, bevor Sie versuchen, das Endpoint Encryption Gerät zu entschlüsseln:

- Verwenden Sie die Reparatur-CD nur dann, wenn das Endpoint Encryption Gerät verschlüsselt ist oder mit der Verschlüsselung begonnen wurde.
- Wenn das Endpoint Encryption Gerät wichtige Daten enthält, fertigen Sie eine Sicherheitskopie an, bevor Sie fortfahren. Anweisungen finden Sie unter http://esupport.trendmicro.com/solution/en-us/1059802.aspx.

- Versuchen Sie nicht, die Festplatte in einem Laptop zu entschlüsseln, es sei denn, er ist an das Stromnetz angeschlossen.
- Wenn die Reparatur-CD nicht gebootet wird, überprüfen Sie, ob auf dem Endpoint Encryption Gerät die neueste BIOS-Version installiert ist. Aktualisieren Sie ggf. das System-BIOS.
- Die Laufwerksentschlüsselung dauert mindestens so lange wie die anfängliche Verschlüsselung.
- Wenn die Reparatur-CD einen fehlerhaften Sektor findet, wird der Prozess deutlich verlangsamt. Führen Sie die Entschlüsselung weiter mit der Reparatur-CD aus, und wenden Sie sich an den Support von Trend Micro, bevor Sie den Prozess unterbrechen.

Warnung!

Unterbrechen Sie den Prozess nicht, nachdem Sie die Entschlüsselung von der Reparatur-CD eingeleitet haben. Es besteht das Risiko von irreversiblen Datenverlusten.

Festplatte mit der Reparatur-CD entschlüsseln

Prozedur

1. Schalten Sie den Endpunkt ein.

   a. Drücken Sie sofort **F12** (oder die entsprechende Taste, um zu den Boot-Optionen zu gelangen).

   b. Legen Sie die Reparatur-CD ein, und wählen Sie im Fenster mit den Boot-Optionen "CD/DVD-Laufwerk".

      Das Gerät bootet und lädt die Umgebung der Reparatur-CD.

Die Preboot-Anmeldung der Full Disk Encryption Reparatur-CD wird angezeigt.

ABBILDUNG 14-7. Preboot der Full Disk Encryption Reparatur-CD

2. Geben Sie den Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Anmelden**.

Das Menüfenster der Full Disk Encryption Reparatur-CD wird angezeigt.

ABBILDUNG 14-8. Full Disk Encryption Reparatur-CD

4. Klicken Sie auf **Wiederherstellungskonsole**.

Das Fenster **Festplatte entschlüsseln** wird angezeigt.

ABBILDUNG 14-9. WIEDERHERSTELLUNGSKONSOLE

5. Klicken Sie auf **Entschlüsseln**, um mit der vollständigen Entschlüsselung des Endpoint Encryption Geräts zu beginnen.

6. Wenn die Entschlüsselung abgeschlossen ist, klicken Sie auf **Beenden**, um zum Menü der Reparatur-CD zurückzukehren.

7. Klicken Sie auf **Computer neu starten**, um das Endpoint Encryption Gerät neu zu starten.

Hinweis

Entfernen Sie die Full Disk Encryption Reparatur-CD aus dem optischen Laufwerk, um das Endpoint Encryption Gerät normal zu starten.

8. Melden Sie sich bei Full Disk Encryption Preboot an.

9. Melden Sie sich bei Windows an, und fahren Sie mit der bevorzugten Wiederherstellungsmethode fort.

Full Disk Encryption Dateien entfernen

Beim Entschlüsseln eines Laufwerks werden MBR-Änderungen und andere wichtige, für den Schutz des Endpoint Encryption Geräts verwendete Elemente entfernt. Wenn Sie Software verschlüsseln, entschlüsseln Sie die Festplatte vollständig, bevor Sie Full Disk Encryption deinstallieren. Andernfalls kommt es auf dem Betriebssystem möglicherweise zu einem kritischen Fehler.

Prozedur

- Gehen Sie an einer Befehlszeile wie folgt vor:

  a. Führen Sie `msiexec.exe /X{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}` aus.

- Aus Windows:

  a. Starten Sie `regedit.exe` aus Windows heraus, und navigieren Sie zu folgendem Schlüssel:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
  \\{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}
  ```

  b. Navigieren Sie zum Schlüssel `UninstallString`:

  Beispiel: `msiexec.exe /x {17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`

  c. Kopieren Sie die Zeichenfolge.

  d. Öffnen Sie den Befehl **Ausführen...** und fügen Sie die Zeichenfolge in das Textfeld **Öffnen** ein.

  e. Klicken Sie auf **OK**.

  Das Fenster **Windows Installer** wird angezeigt.

f. Wenn die Deinstallationsbestätigung angezeigt wird, klicken Sie auf **Ja**.

Hinweis

Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Zulassen**.

g. Wenn Sie aufgefordert werden, DrAService zu beenden, wählen Sie das zweite Optionsfeld **Anwendungen nicht schließen**, und klicken Sie anschließend auf **OK**.

h. Wenn Sie dazu aufgefordert werden, den Endpunkt neu zu starten, klicken Sie auf **Ja**. Starten Sie andernfalls den Endpunkt manuell neu.

Patch-Verwaltung mit Full Disk Encryption

Verwenden Sie Command Line Helper zusammen mit DAAutoLogin zur Ausführung der Windows Patch-Verwaltung auf Geräten, auf denen Full Disk Encryption installiert ist. Command Line Helper erstellt verschlüsselte Werte für Skripts und DAAutoLogin ermöglicht das einmalige Umgehen von Full Disk Encryption Preboot.

DAAutoLogin bietet je nach Anforderung mehrere Anwendungsmöglichkeiten. Sie können Patches per Push-Verfahren senden, gefolgt von einem Skript mit DAAutoLogin, das einen Befehl zum Neustarten an das Gerät sendet. Auf dem Gerät wird dann Windows GINA angezeigt und die erfolgreiche Durchführung des Patching bestätigt oder es können weitere Patches bereitgestellt werden.

DAAutoLogin akzeptiert die folgenden Switches:

```
DAAutoLogin <Preboot-Benutzername> <Preboot-Kennwort>
[<Domänenname> <Domänenbenutzername> <Domänenkennwort>]
```

Sie können alle erforderlichen Werte übergeben und durch ein Leerzeichen trennen. Wenn Sie die Parameter zur Domäne hinzufügen, ermöglichen Sie die Windows Authentifizierung.

Hinweis

- Vergewissern Sie sich, dass beide Tools auf einem Gerät ausgeführt werden, auf dem Full Disk Encryption installiert ist.
- Beide Tools befinden sich im Ordner "Tools" in der ZIP-Datei, die Sie von Trend Micro erhalten haben. Hilfe erhalten Sie beim Support von Trend Micro.

Command Line Helper

Administratoren können mit Command Line Helper zusammen mit DAAutoLogin eine problemlose Patch-Verwaltung mit Full Disk Encryption durchführen. Mit Command Line Helper können Sie über ein Installationsskript verschlüsselte Werte an Full Disk Encryption Preboot übergeben. `DAAutoLogin` lässt das einmalige Umgehen von Full Disk Encryption Preboot zu.

Prozedur

1. Kopieren Sie `CommandLineHelper.exe` auf die lokale Festplatte des Computers, auf dem Full Disk Encryption installiert ist.

   Beispiel: Kopieren Sie `CommandLineHelper.exe` auf das Laufwerk `C:\`.

2. Öffnen Sie ein Eingabeaufforderungsfenster, geben Sie `C:\CommandLineHelper.exe` ein, und geben Sie anschließend den Benutzernamen oder das Kennwort ein.

   Wenn der Benutzername beispielsweise "SMSUser" ist, geben Sie folgenden Befehl ein:

   ```
   C:\CommandLineHelper.exe SMSUser
   ```

3. Drücken Sie die EINGABETASTE, um den verschlüsselten Wert anzuzeigen.

4. Führen Sie Command Line Helper erneut aus, um den zweiten Wert zu verschlüsseln. Falls Sie zunächst den Benutzernamen verschlüsselt haben, verschlüsseln Sie im zweiten Durchgang das Kennwort.

Patching-Verfahren für Full Disk Encryption

Prozedur

1. Sie können Patch-Dateien auf bestimmte Full Disk Encryption Geräte übertragen.
2. Senden Sie ein Skript, das `DAAutoLogin` ausführt.
3. Senden Sie einen Befehl zum Neustarten, so dass das Full Disk Encryption Gerät Windows GINA lädt und die erfolgreiche Durchführung des Patching bestätigt oder um weitere Patches per Push-Verfahren zu senden.

Kapitel 15

Encryption Management für Fremdprodukte

Eine Hauptfunktion von Full Disk Encryption ist die Fähigkeit, Verschlüsselungsprodukte von Fremdherstellern zu verwalten. Die Endpoint Encryption Agents können vollständig in die Verschlüsselungslösungen integriert werden, die Teil des Host-Betriebssystems sind.

Es werden folgende Themen behandelt:

- *Info über Agents zur Encryption Management auf Seite 15-2*
- *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 15-3*
- *Encryption Management for Microsoft BitLocker auf Seite 15-5*
- *Encryption Management for Apple FileVault auf Seite 15-11*

Info über Agents zur Encryption Management

In der folgenden Tabelle werden die beiden Full Disk Encryption Agents für die Verschlüsselungsverwaltung von Produkten von Fremdherstellern erläutert.

Hinweis

Informationen zu allen verfügbaren Endpoint Encryption Agents finden Sie unter *Endpoint Encryption Agents auf Seite 1-18*.

TABELLE 15-1. Agents zur Encryption Management

AGENT	BESCHREIBUNG
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.

Einschränkungen der Agent-Richtlinie der Encryption Management

In der folgenden Tabelle werden die Richtlinieneinschränkungen für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker beschrieben. Um alle Richtlinien zu verwalten, installieren Sie stattdessen den Full Disk Encryption Agent.

Hinweis

Die Encryption Management for Microsoft BitLocker und die Encryption Management for Apple FileVault erfordern keine Authentifizierung und werden nicht durch Authentifizierungsrichtlinien beeinflusst. Client, Anmeldung, Kennwort und Authentifizierungsrichtlinien oder die Berechtigung des Benutzers, die Endpoint Encryption Agent-Software zu deinstallieren, wirkt sich nur auf die Full Disk Encryption Agents und File Encryption Agents aus.

In der folgenden Tabelle werden die Richtlinien beschrieben, die sich auf jeden Agent auswirken. Anhand der Tabelle können Sie die Richtlinieneinschränkungen bei Agents von Fremdherstellern verstehen.

TABELLE 15-2. Richtlinien, die sich auf Full Disk Encryption Agents auswirken

RICHTLINIE	FULL DISK ENCRYPTION	ENCRYPTION MANAGEMENT FOR APPLE FILEVAULT	ENCRYPTION MANAGEMENT FOR MICROSOFT BITLOCKER
Wiederherstellung durch Benutzer zulassen	●		
Deinstallation durch Benutzer zulassen	●		
Gerät verschlüsseln	●	●	●
Kontosperraktion	●		

Richtlinie	Full Disk Encryption	Encryption Management for Apple FileVault	Encryption Management for Microsoft BitLocker
Zeitraum bis Kontosperrung	●		
Kennwort zur Auslöschung	●		
Aktion zur Gerätesperrung	●		
Aktion zur Auslöschung des Geräts	●	●	●
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	●		
Falls gefunden	●		
Rechtlicher Hinweis	●	●	●
Zeitverzögerung bei Gerätesperre	●		
Preboot-Umgehung	●		
Support-Informationen	●		
Token-Authentifizierung	●		
Zulässige Authentifizierungsmethoden	●		
Synchronisierungsintervall	●	●	●

Encryption Management for Microsoft BitLocker

Die Encryption Management for Microsoft BitLocker verwaltet die BitLocker-Laufwerksverschlüsselung™ (BDE) für Endpunkte, auf denen die Betriebssysteme Microsoft Windows 7 Ultimate und Enterprise und Windows 8 Pro und Enterprise ausgeführt werden. Die Encryption Management for Microsoft BitLocker schützt Daten durch die Verschlüsselung ganzer Volumes. Standardmäßig verwendet BDE den AES-Verschlüsselungsalgorithmus im CBC-Modus mit einem 128-Bit- oder 256-Bit-Schlüssel.

Status der Verschlüsselung anzeigen

Prozedur

1. Klicken Sie auf das Full Disk Encryption Symbol ( ).
   - Unter Windows wechseln Sie in die Task-Leiste.
   - Unter Mac OS wechseln Sie zur Menüleiste.
2. Öffnen Sie die Registerkarte **Verschlüsselungsstatus**.
3. Weitere Informationen finden Sie unter *Grundlegendes zum Verschlüsselungsstatus auf Seite 15-5*.

Grundlegendes zum Verschlüsselungsstatus

Auf der Registerkarte **Verschlüsselungsstatus** finden Sie Details zu den verschlüsselten Laufwerken, den Verschlüsselungstypen und dem Verhältnis zwischen

verschlüsselten und nicht verschlüsselten Anteilen auf dem Laufwerk. Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

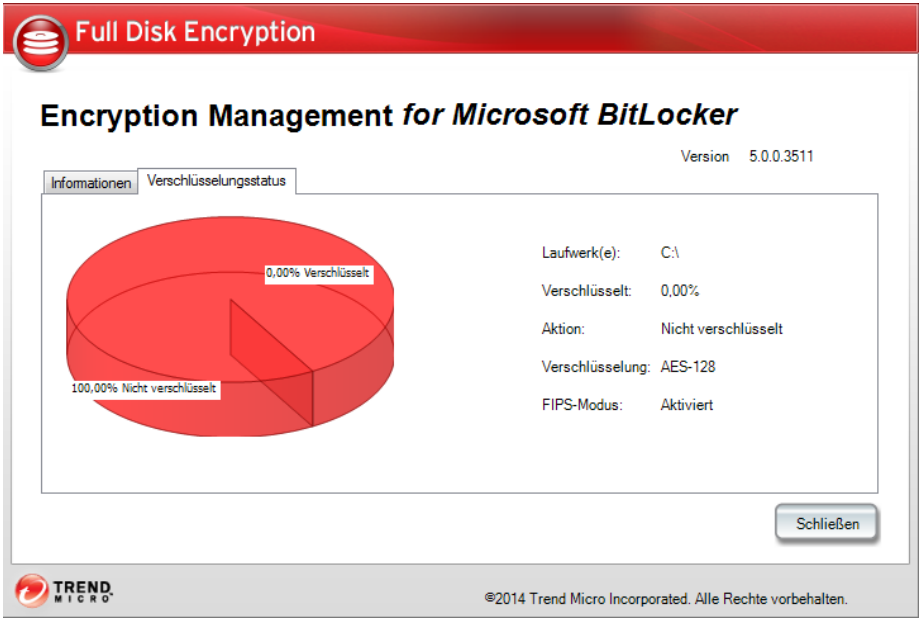


TABELLE 15-3. Geräteverschlüsselungsstatus

VORGANG	BESCHREIBUNG
Kreisdiagramm	Das Kreisdiagramm stellt das Verhältnis dar, in dem die Festplatte verschlüsselt und nicht verschlüsselt ist.
Laufwerk	Die Festplatte mit installiertem Agent.
Verschlüsselt	Der Prozentsatz der Verschlüsselung des Laufwerks.
Aktion	Der aktuelle Verschlüsselungsstatus.

VORGANG	BESCHREIBUNG
Verschlüsselung	Die Art der Verschlüsselung auf dem Endpunkt. **Hinweis** Die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker verwenden immer die Software-basierte Verschlüsselung.
FIPS-Modus	Gibt an, ob FIPS aktiviert ist. Weitere Informationen zu FIPS finden Sie unter *Info über FIPS auf Seite 1-9*.

Grundlegendes zu Agent-Informationen

Auf der Registerkarte **Informationen** finden Sie ausführliche Informationen zum Benutzerkonto, zum Endpoint Encryption Gerät und zur Richtliniensynchronisierung.

Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

Full Disk Encryption
Encryption Management for Microsoft BitLocker
Version 5.0.0.3511
Informationen
Verschlüsselungsstatus
TMEE Benutzername: admin
Geräte-ID: bfebfbff-0000-06fd-001c-bf8bd9af0000
Betriebssystem: Microsoft Windows 7 Ultimate
Nom de l'ordinateur: DE-PC
Letzte Synchronisierung: 28.05.2014 05:04:14
Mit PolicyServer synchronisieren
Achtung: Dieses Computerprogramm ist urheberrechtlich und durch internationale Verträge geschützt. Unbefugte Vervielfältigung oder unbefugter Vertrieb dieses Programms oder eines Teils davon sind strafbar. Dies wird sowohl straf- als auch zivilrechtlich verfolgt und kann schwere Strafen und Schadensersatzforderungen zur Folge haben.
Schließen
TREND MICRO
©2014 Trend Micro Incorporated. Alle Rechte vorbehalten.

TABELLE 15-4. Agent-Informationen

BEZEICHNUNG	BESCHREIBUNG
TMEE Benutzername	Das zur Anmeldung beim Endpoint Encryption Gerät verwendete Endpoint Encryption Konto. Dabei handelt es sich um ein anderes Konto als für die Windows-Anmeldung.
Geräte-ID	Die eindeutige ID, die den Agent und den Endpunkt für PolicyServer identifiziert.
Betriebssystem	Das momentan auf dem Endpunkt installierte Betriebssystem, einschließlich der Version.
Computername	Der Name, mit dem der Endpunkt-Computer im Netzwerk identifiziert wird.

Bezeichnung	Beschreibung
Letzte Synchronisierung	Der Zeitstempel für die letzte Richtliniensynchronisierung mit PolicyServer. Weitere Informationen zur Synchronisierung von Richtlinien finden Sie unter *Richtlinien über die Menüleiste synchronisieren auf Seite 15-16*.
Mit PolicyServer synchronisieren	Erzwingt eine unverzügliche Aktualisierung der Richtlinien.

Richtlinien mit PolicyServer synchronisieren

Es gibt zwei Methoden, um Richtlinien mit PolicyServer zu synchronisieren. Informationen zu Richtlinien, die sich auf Geräte mit der Encryption Management for Microsoft BitLocker auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 15-3*.

- *Richtlinien über die Menüleiste synchronisieren auf Seite 15-16*
- *Richtlinien über das Fenster "Info" synchronisieren auf Seite 15-10*

Automatische Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Endpoint Encryption Agents und PolicyServer einleiten.

- Nachdem das Betriebssystem geladen wird und der Dienst des Endpoint Encryption Agent startet

  Hinweis

  Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- Wenn Full Disk Encryption Preboot startet (nur Full Disk Encryption)
- Die Zeitdauer der Richtlinie **Synchronisierungsintervall** läuft ab

Öffnen Sie das Fenster **Info über**, um Endpoint Encryption Agent anzuweisen, die Richtlinien manuell zu synchronisieren.

Hinweis

Aktionen für Endpoint Encryption Geräte werden eingeleitet, nachdem der Endpoint Encryption Agent Richtlinien-Updates erhält.

Richtlinien über das Fenster "Info" synchronisieren

Informationen zu Richtlinieneinschränkungen, die sich auf die Encryption Management for Microsoft BitLocker Agent auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 15-3*.

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Info über Full Disk Encryption**, um das Menü des Agent zu öffnen.
4. Öffnen Sie die Registerkarte **Informationen**.
5. Klicken Sie auf **Mit PolicyServer synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Richtlinien über die Task-Leiste synchronisieren

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Mit PolicyServer synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Encryption Management for Apple FileVault

Die Encryption Management for Apple FileVault verwaltet Apple Filevault™ zum Verschlüsseln des gesamten OS X-Startvolumes, das normalerweise das Home-Verzeichnis enthält. Auf diese Weise kann auf Datenträger-Images verzichtet werden. Die Encryption Management for Apple FileVault verwaltet die Verschlüsselung mit Apple FileVault, wobei das Kennwort des Benutzers als Passphrase für die Verschlüsselung verwendet wird. Die Encryption Management for Apple FileVault verwendet den AES-XTS-Modus von AES mit 128-Bit-Blöcken und einem 256-Bit-Schlüssel zur Verschlüsselung des Datenträgers entsprechend der NIST-Empfehlung. Nur Benutzer mit der Berechtigung, Laufwerke zu entsperren, können das Laufwerk starten und entsperren. Einmal entsperrt, können Benutzer den Computer auch nutzen, bis dieser heruntergefahren wird.

Hinweis

Lokale Mac OS-Konten oder mobile Konten können die Verschlüsselung unter Mac OS X Mountain Lion oder höher einleiten. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten.

Informationen darüber, wie Sie ein mobiles Konto für Active Directory auf dem Mac einrichten, finden Sie unter *Mobiles Konto für Active Directory unter Mac OS erstellen auf Seite 15-17*.

Status der Verschlüsselung anzeigen

Prozedur

1. Klicken Sie auf das Full Disk Encryption Symbol ( ).
   - Unter Windows wechseln Sie in die Task-Leiste.
   - Unter Mac OS wechseln Sie zur Menüleiste.
2. Öffnen Sie die Registerkarte **Verschlüsselungsstatus**.

3. Weitere Informationen finden Sie unter *Grundlegendes zum Verschlüsselungsstatus auf Seite 15-5*.

Grundlegendes zum Verschlüsselungsstatus

Auf der Registerkarte **Verschlüsselungsstatus** finden Sie Details zu den verschlüsselten Laufwerken, den Verschlüsselungstypen und dem Verhältnis zwischen verschlüsselten und nicht verschlüsselten Anteilen auf dem Laufwerk. Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

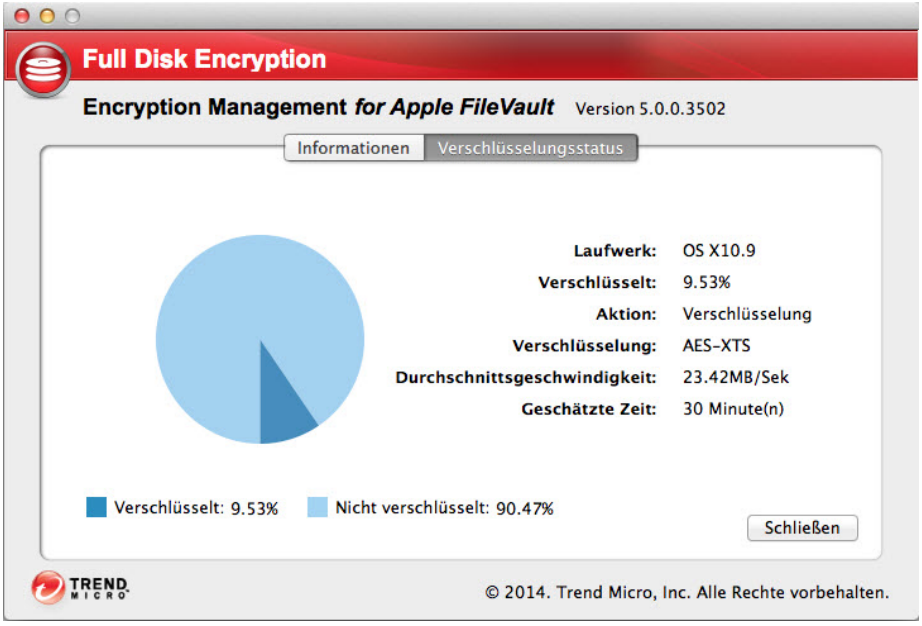


TABELLE 15-5. Geräteverschlüsselungsstatus

VORGANG	BESCHREIBUNG
Kreisdiagramm	Das Kreisdiagramm stellt das Verhältnis dar, in dem die Festplatte verschlüsselt und nicht verschlüsselt ist.

Vorgang	Beschreibung
Laufwerk	Die Festplatte mit installiertem Agent.
Verschlüsselt	Der Prozentsatz der Verschlüsselung des Laufwerks.
Aktion	Der aktuelle Verschlüsselungsstatus.
Durchschnittsgeschwindigkeit	Die Rate (MB/Sekunden), mit der das Laufwerk verschlüsselt oder entschlüsselt wird.
Geschätzte Zeit	Die Zeitdauer, bis das Laufwerk vollständig verschlüsselt oder entschlüsselt wurde.

Grundlegendes zu Agent-Informationen

Auf der Registerkarte **Informationen** finden Sie ausführliche Informationen zum Benutzerkonto, zum Endpoint Encryption Gerät und zur Richtliniensynchronisierung.

Weitere Informationen finden Sie im nachfolgenden Diagramm und in der Beschreibung.

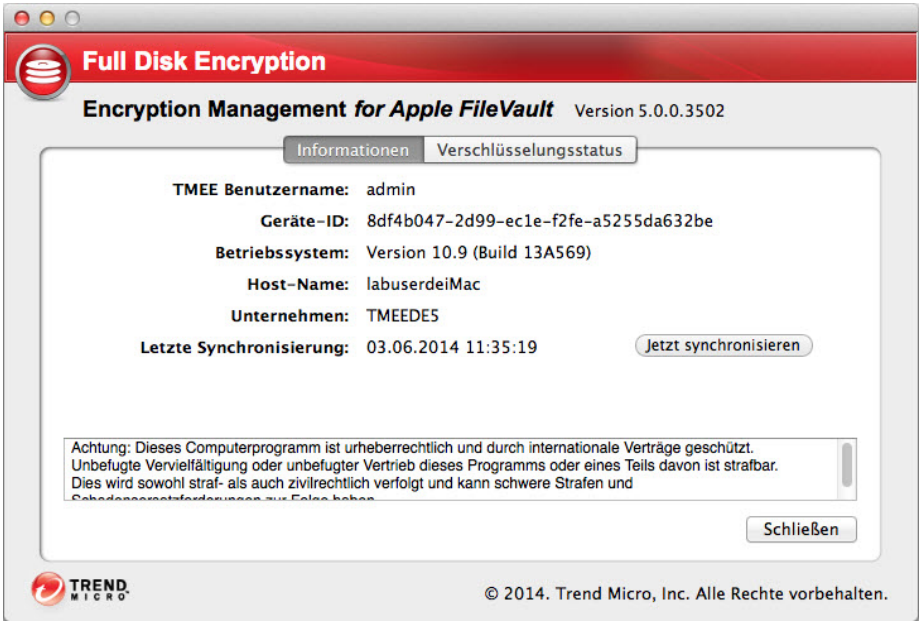


TABELLE 15-6. Agent-Informationen

BEZEICHNUNG	BESCHREIBUNG
TMEE Benutzername	Das zur Anmeldung beim Endpoint Encryption Gerät verwendete Endpoint Encryption Konto. Dabei handelt es sich um ein anderes Konto als für die Windows-Anmeldung.
Geräte-ID	Die eindeutige ID, die den Agent und den Endpunkt für PolicyServer identifiziert.
Betriebssystem	Das momentan auf dem Endpunkt installierte Betriebssystem, einschließlich der Version.

Bezeichnung	Beschreibung
Computername	Der Name, mit dem der Endpunkt-Computer im Netzwerk identifiziert wird.
Unternehmen	Der Unternehmensname des PolicyServer, der die Agent-Richtlinien verwaltet.
Letzte Synchronisierung	Der Zeitstempel für die letzte Richtliniensynchronisierung mit PolicyServer. Weitere Informationen zur Synchronisierung von Richtlinien finden Sie unter *Richtlinien über die Menüleiste synchronisieren auf Seite 15-16*.
Jetzt synchronisieren	Erzwingt eine unverzügliche Aktualisierung der Richtlinien.

Richtlinien mit PolicyServer synchronisieren

Es gibt zwei Methoden, um Richtlinien mit PolicyServer zu synchronisieren. Informationen zu Richtlinien, die sich auf Geräte mit der Encryption Management for Apple FileVault auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 15-3*.

- *Richtlinien über das Fenster "Info" synchronisieren auf Seite 15-16*
- *Richtlinien über die Menüleiste synchronisieren auf Seite 15-16*

Automatische Synchronisierung von Richtlinien

In der folgenden Liste werden die Ereignisse beschrieben, die die Richtliniensynchronisierung zwischen allen Endpoint Encryption Agents und PolicyServer einleiten.

- Nachdem das Betriebssystem geladen wird und der Dienst des Endpoint Encryption Agent startet

Hinweis

Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

- Wenn Full Disk Encryption Preboot startet (nur Full Disk Encryption)
- Die Zeitdauer der Richtlinie **Synchronisierungsintervall** läuft ab

Öffnen Sie das Fenster **Info über**, um Endpoint Encryption Agent anzuweisen, die Richtlinien manuell zu synchronisieren.

Hinweis

Aktionen für Endpoint Encryption Geräte werden eingeleitet, nachdem der Endpoint Encryption Agent Richtlinien-Updates erhält.

Richtlinien über das Fenster "Info" synchronisieren

Informationen zu Richtlinieneinschränkungen, die sich auf die Encryption Management for Apple FileVault Agents auswirken, finden Sie unter *Einschränkungen der Agent-Richtlinie der Encryption Management auf Seite 15-3*.

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).
3. Wählen Sie **Info über Full Disk Encryption**, um das Menü des Agent zu öffnen.
4. Öffnen Sie die Registerkarte **Informationen**.
5. Klicken Sie auf **Jetzt synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Richtlinien über die Menüleiste synchronisieren

Prozedur

1. Vergewissern Sie sich, dass das Endpoint Encryption Gerät Netzwerkzugriff hat.
2. Klicken Sie auf das Agent-Symbol ( ).

3. Wählen Sie **Richtlinien synchronisieren**.

Bei Erfolg sind alle Endpoint Encryption Richtlinien aktuell.

Mobiles Konto für Active Directory unter Mac OS erstellen

Lokale Mac OS-Konten oder mobile Konten können die Verschlüsselung unter Mac OS X Mountain Lion oder höher einleiten. Andere Mac OS-Benutzerkontentypen sind nicht in der Lage, die Verschlüsselung einzuleiten.

Wenn ein anderes Mac OS-Konto als ein lokales oder mobiles Konto versucht, eine Verschlüsselung einzuleiten, wird die folgende Meldung angezeigt:

Full Disk Encryption erfordert Authentifizierung
Geben Sie das Kennwort für das aktuell angemeldete Benutzerkonto ein, und starten Sie den Endpunkt anschließend neu, um die Verschlüsselung zu starten.
Mit dem Kontotyp des aktuellen Benutzerkontos kann die Verschlüsselung nicht gestartet werden. Melden Sie sich bei einem lokalen oder mobilen Konto an, und versuchen Sie es erneut.
Abbrechen
Neu starten

Die folgende Aufgabe zeigt, wie Sie ein mobiles Konto für Ihr Mac OS-Konto erstellen, um dieses Problem zu umgehen.

Prozedur

1. Navigieren Sie im Apple-Menü zu **Systemeinstellungen...**.

   Das Fenster **Systemeinstellungen** wird angezeigt.

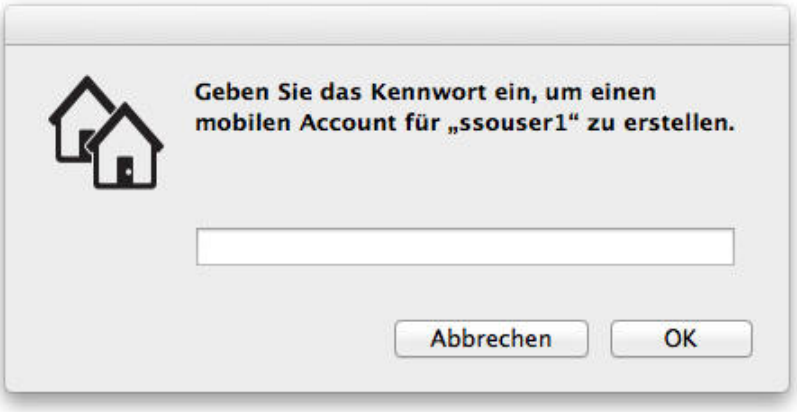
2. Wählen Sie **Benutzergruppen** im Abschnitt **System**.

3. Klicken Sie in der unteren linken Ecke auf das Sperrsymbol.

4. Klicken Sie auf **Erstellen...** neben **Mobiles Konto**.

5. Wählen Sie in den folgenden Fenster die persönlichen Einstellungen, und klicken Sie auf **Erstellen**, um zum jeweils nächsten Fenster zu gelangen.

6. Wenn Sie dazu aufgefordert werden, geben Sie Ihr Active Directory-Kennwort ein, und klicken Sie auf **OK**.



Ihr mobiles Konto wurde erstellt. Sie können nun mit diesem mobilen Konto die Verschlüsselung einleiten.

Teil V

Erweiterte Verwaltung und technischer Support

Kapitel 16

Erweiterte Unternehmensfunktionen

In Umgebungen, die hauptsächlich von Control Manager verwaltet werden, setzen Sie PolicyServer MMC für erweiterte Optionen ein, einschließlich bestimmter Berichte, Protokolle und Wartung. Endpoint Encryption erstellt umfassende Protokolle und generiert Berichte über Ereignisse und Aktualisierungen. Mit Hilfe von Protokollen und Berichten können Sie die Richtliniensteuerung bewerten und die Gültigkeit von Komponenten-Updates überprüfen. Die Unternehmenswartung bietet Methoden, um inaktive Benutzer und Geräte endgültig zu löschen. Ferner werden übereinstimmende Kriterien aus der Datenbank protokolliert.

Es werden folgende Themen behandelt:

- *Unternehmen - Wartung auf Seite 16-2*
- *Gelöschte Benutzer und Geräte wiederherstellen auf Seite 16-11*
- *Unternehmen - Protokollereignisse auf Seite 16-12*
- *Unternehmen - Berichte auf Seite 16-17*

Unternehmen - Wartung

PolicyServer zeichnet Systemaktivitäten (an Richtlinien vorgenommene Änderungen, erfolgreiche Authentifizierungsverusche, aufgrund von nicht erfolgreichen Anmeldeversuchen gesperrte Geräte) auf und verwaltet diese Datensätze als Protokollereignisse. Sie können Berichte bei Bedarf oder zeitgesteuert generieren.

PolicyServer MMC verfügt über eine Vielzahl an integrierten Berichten, um den Status der Geräteverschlüsselung, die Aktivität von Benutzern oder Geräten und die PolicyServer Integrität zu überprüfen.

Hinweis

Nur Konten mit der Benutzerrolle Unternehmensadministrator können Berichte verwenden.

Inaktive Benutzer löschen

Bei einem inaktiven Benutzer handelt es sich um ein Benutzerkonto, das während einer bestimmten Zeit bei keinem der Endpoint Encryption Geräte angemeldet war.

Über den Knoten "Unternehmen - Wartung" in PolicyServer MMC können Sie inaktive Endpoint Encryption Benutzer und Geräte endgültig löschen. Anschließend können Sie die Protokollereignisse des endgültig gelöschten Benutzers oder endgültig gelöschten Geräts anzeigen. Zusätzlich können Sie bestimmte Kriterien zum endgültigen Löschen der Protokolldatenbank zu einer bestimmten Zeit oder entsprechend einem Zeitplan festlegen.

Warnung!

Mit endgültig gelöschten Benutzerkonten kann keine Authentifizierung bei Endpoint Encryption Geräten erfolgen.

Inaktive Benutzer endgültig löschen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.
3. Klicken Sie auf **Inaktive Benutzer löschen**.
4. Geben Sie die Anzahl der Tage ein, nach denen alle Benutzerkonten endgültig gelöscht werden, die sich seit dieser Zeit nicht bei einem Gerät angemeldet haben.

   Hinweis

   Geben Sie einen Bereich zwischen 7 und 999 Tagen ein.

5. Klicken Sie auf **Endgültig löschen**.
6. Klicken Sie auf **OK**, um die endgültige Löschung zu bestätigen.

Alle Daten, die die Kriterien zur endgültigen Löschen erfüllen, werden aus der Datenbank gelöscht.

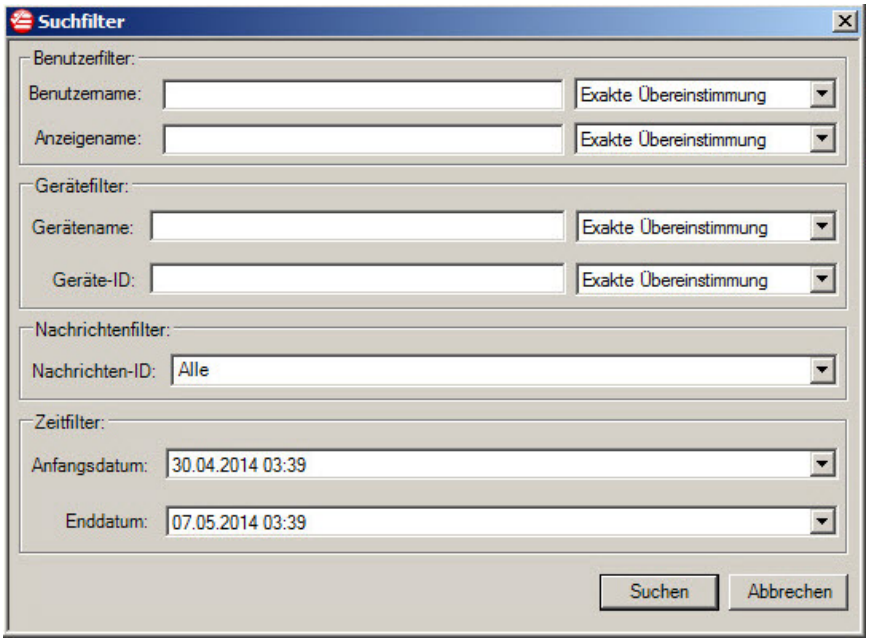
Protokollereignis zum endgültigen Löschen inaktiver Benutzer anzeigen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Klicken Sie auf **Unternehmen - Protokollereignisse**.

   Im rechten Fensterbereich werden alle aktuellen Protokollereignisse angezeigt.
3. Klicken Sie unten auf der Seite auf **Filter**.

Das Fenster **Suchfilter** wird angezeigt.



4. Wählen Sie aus dem Listenfeld **Nachrichten-ID 200105, Aus dem Unternehmen entfernte inaktive Benutzer**.

5. Klicken Sie auf **Suchen**.

   Alle Protokollereignisse, die den angegebenen Kriterien entsprechen, werden angezeigt.

6. Doppelklicken Sie auf ein Protokollereignis.

   Das Fenster **Protokolldatensatz** wird mit allen Protokolldaten für das ausgewählte Ereignis angezeigt.

Bericht zum endgültigen Löschen inaktiver Benutzer anzeigen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.
3. Klicken Sie auf **Unternehmen - Zeitgesteuerte Berichte**.
4. Gehen Sie im rechten Fensterbereich wie folgt vor:
   - Um den Bericht im Tabellenformat anzuzeigen, doppelklicken Sie auf **Inaktive Benutzer wurden gelöscht**.
   - Um den Bericht im HTML-Format anzuzeigen, klicken Sie mit der rechten Maustaste auf einen Bericht, und wählen Sie anschließend **Bericht anzeigen**.

Inaktive Geräte löschen

Bei einem inaktiven Gerät handelt es sich um ein Endpoint Encryption Gerät, bei dem sich während einer bestimmten Zeit niemand angemeldet hat.

Über den Knoten "Unternehmen - Wartung" in PolicyServer MMC können Sie inaktive Endpoint Encryption Benutzer und Geräte endgültig löschen. Anschließend können Sie die Protokollereignisse des endgültig gelöschten Benutzers oder endgültig gelöschten Geräts anzeigen. Zusätzlich können Sie bestimmte Kriterien zum endgültigen Löschen der Protokolldatenbank zu einer bestimmten Zeit oder entsprechend einem Zeitplan festlegen.

Warnung!

Benutzer können sich nicht bei endgültig gelöschten Endpoint Encryption Geräten anmelden.

Inaktive Geräte endgültig löschen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.
3. Klicken Sie auf **Inaktive Geräte löschen**.
4. Geben Sie die Anzahl der Tage ein, nach denen alle Benutzerkonten endgültig gelöscht werden, die sich seit dieser Zeit nicht bei einem Endpoint Encryption Gerät angemeldet haben.
5. Klicken Sie auf **Endgültig löschen**.
6. Klicken Sie auf **OK**, um die endgültige Löschung zu bestätigen.

Alle Daten, die die Kriterien zur endgültigen Löschen erfüllen, werden aus der Datenbank gelöscht.

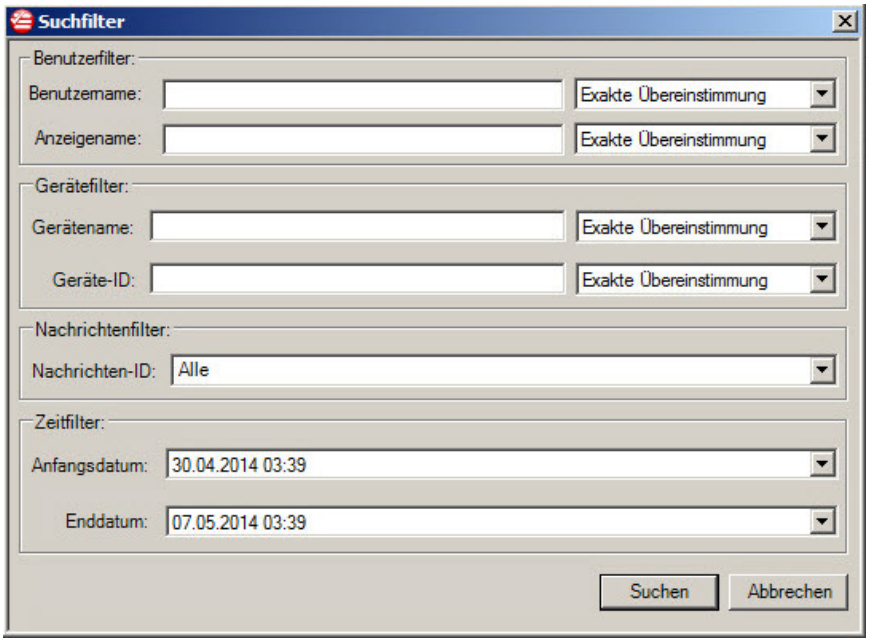
Protokollereignis zum endgültigen Löschen inaktiver Geräte anzeigen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Klicken Sie auf **Unternehmen - Protokollereignisse**.

   Im rechten Fensterbereich werden alle aktuellen Protokollereignisse angezeigt.
3. Klicken Sie unten auf der Seite auf **Filter**.

Das Fenster **Suchfilter** wird angezeigt.



4. Wählen Sie aus dem Listenfeld **Nachrichten-ID 200303, Aus dem Unternehmen entfernte inaktive Geräte**.

5. Klicken Sie auf **Suchen**.

   Alle Protokollereignisse, die den angegebenen Kriterien entsprechen, werden angezeigt.

6. Doppelklicken Sie auf ein Protokollereignis.

   Das Fenster **Protokolldatensatz** wird mit allen Protokolldaten für das ausgewählte Ereignis angezeigt.

Bericht über gelöschte inaktive Geräte anzeigen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.
3. Klicken Sie auf **Unternehmen - Zeitgesteuerte Berichte**.
4. Gehen Sie im rechten Fensterbereich wie folgt vor:
   - Um den Bericht im Tabellenformat anzuzeigen, doppelklicken Sie auf **Inaktive Geräte wurden gelöscht**.
   - Um den Bericht im HTML-Format anzuzeigen, klicken Sie mit der rechten Maustaste auf einen Bericht, und wählen Sie anschließend **Bericht anzeigen**.

Der Bericht wird angezeigt.

Protokoll endgültig löschen

Über den Knoten "Unternehmen - Wartung" in PolicyServer MMC können Sie inaktive Endpoint Encryption Benutzer und Geräte endgültig löschen. Anschließend können Sie die Protokollereignisse des endgültig gelöschten Benutzers oder endgültig gelöschten Geräts anzeigen. Zusätzlich können Sie bestimmte Kriterien zum endgültigen Löschen der Protokolldatenbank zu einer bestimmten Zeit oder entsprechend einem Zeitplan festlegen.

Die Protokolldatenbank endgültig löschen

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.

3. Klicken Sie auf **Protokolldatenbank bereinigen**.
4. Wählen Sie **Zeitgesteuerte Bereinigung aktivieren**.
5. Konfigurieren Sie die folgenden Optionen:

Option	Bezeichnung
Protokolle bereinigen, die älter als <X> Tage sind	Geben Sie die Anzahl der Tage ein, die Protokolle archiviert werden. Protokolle, die älter sind als die angegebene Anzahl von Tagen, werden bereinigt.
Intervalltyp	Sie können festlegen, dass die Protokolldatenbank täglich, wöchentlich, alle zwei Wochen oder monatlich bereinigt wird.
Anfangsdatum	Wählen Sie, wann die zeitgesteuerte Bereinigung beginnen soll.
Zeit	Geben Sie die Tageszeit für die zeitgesteuerte Bereinigung ein.

6. Klicken Sie auf **Übernehmen**.
7. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Alle Daten, die die Kriterien zur endgültigen Löschen erfüllen, werden aus der Datenbank gelöscht.

Ereignis "Protokolldatenbank bereinigen" anzeigen

Hinweis

Die Protokolldatenbank wird nur bereinigt, wenn die Kriterien für die zeitgesteuerte Bereinigung erfüllt werden. Wenn keine Daten den Suchkriterien entsprechen, überprüfen Sie, ob der Zeitplan richtig eingerichtet wurde. Weitere Informationen finden Sie unter *Die Protokolldatenbank endgültig löschen auf Seite 16-8*.

Prozedur

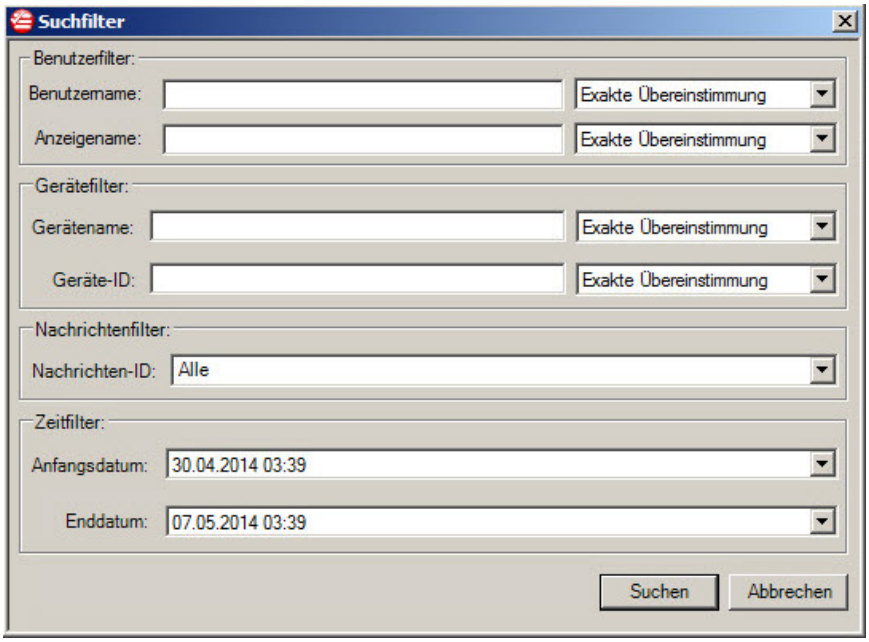
1. Melden Sie sich bei PolicyServer MMC an.

2. Klicken Sie auf **Unternehmen - Protokollereignisse**.

   Im rechten Fensterbereich werden alle aktuellen Protokollereignisse angezeigt.

3. Klicken Sie unten auf der Seite auf **Filter**.

   Das Fenster **Suchfilter** wird angezeigt.



4. Wählen Sie aus dem Listenfeld **Nachrichten-ID** den Eintrag **103104, Aus dem Unternehmen gelöschte Protokolldaten**.

5. Klicken Sie auf **Suchen**.

   Alle Protokollereignisse, die den angegebenen Kriterien entsprechen, werden angezeigt.

6. Doppelklicken Sie auf ein Protokollereignis.

Das Fenster **Protokolldatensatz** wird mit allen Protokolldaten für das ausgewählte Ereignis angezeigt.

Gelöschte Benutzer und Geräte wiederherstellen

Mit dem Papierkorb von PolicyServer MMC stellen Sie gelöschte Endpoint Encryption Benutzer oder Geräte wieder her. Alle gelöschten Endpoint Encryption Benutzer und Geräte werden auf Unternehmensebene im Papierkorb gesichert. Gruppen haben keinen Papierkorb. Wiederhergestellte gelöschte Endpoint Encryption Benutzer oder Geräte werden nicht automatisch der zuvor zugewiesenen Richtliniengruppe hinzugefügt.

Gelöschtes Benutzer wiederherstellen

In Umgebungen mit Control Manager und PolicyServer MMC können Sie gelöschte Endpoint Encryption Benutzer mit dem Papierkorb-Knoten von PolicyServer MMC wiederherstellen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie den **Papierkorb**.
3. Öffnen Sie **Gelöschte Benutzer**.

   Im rechten Fenster werden alle gelöschten Benutzer geladen.
4. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto, und wählen Sie anschließend **Benutzer wiederherstellen**.

   Der Benutzer wird wieder zum Unternehmen hinzugefügt, gehört jedoch keiner Richtliniengruppe an.

Gelöschtes Gerät wiederherstellen

Im Umgebungen mit Control Manager und PolicyServer MMC können Sie gelöschte Endpoint Encryption Geräte mit dem Papierkorb-Knoten von PolicyServer MMC wiederherstellen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Erweitern Sie das Unternehmen, navigieren Sie anschließend zu **Unternehmen - Wartung**.
3. Erweitern Sie den **Papierkorb**.
4. Öffnen Sie **Gelöschte Geräte**.

   Im rechten Fensterbereich werden alle gelöschten Endpoint Encryption Geräte angezeigt.
5. Klicken Sie mit der rechten Maustaste auf das Endpoint Encryption Gerät, und wählen Sie anschließend **Gerät wiederherstellen**.

   Das Endpoint Encryption Gerät wird wieder zum Unternehmen hinzugefügt, gehört jedoch keiner Richtliniengruppe an.

Unternehmen - Protokollereignisse

PolicyServer zeichnet Protokollereignisse unter Verwendung vordefinierter Kriterien auf, wie z. B. Zugriffsversuche, Systemfehler, Änderungen an Benutzern oder Gruppen, Richtlinienänderungen sowie Probleme bei der Einhaltung von Richtlinien. Durch die Verwaltung von Protokollereignissen und Berichten können der Unternehmensadministrator und der Gruppenadministrator nach speziellen Protokollereignissen und Berichten über Server- und Client-Sicherheit suchen.

Protokollereignisse verwalten

Nur Nachrichten der letzten sieben Tage werden automatisch angezeigt. Verwenden Sie den Filter, um ältere Protokollereignisse anzuzeigen. Es ist nützlich, die Protokolle anhand der Nachrichten-ID zu durchsuchen. Wenn Sie beispielsweise nach der Nachrichten-ID „400008“ suchen, werden alle Nachrichten vom Typ „Geräteverschlüsselung abgeschlossen“ angezeigt. Informationen zu Nachrichten-IDs finden Sie unter *PolicyServer Nachrichten-IDs auf Seite B-1*.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Wählen Sie eine Protokollereignisstufe aus:
   - Für Protokolle auf Unternehmensebene erweitern Sie **Unternehmen - Protokollereignisse**.
   - Für Protokolle auf Gruppenebene navigieren Sie zu **Gruppenname** > **Protokollereignisse.**

   Das Fenster "Protokoll" wird angezeigt. Alle Ereignisse der letzten sieben (7) Tage werden automatisch angezeigt.
3. Doppelklicken Sie auf ein beliebiges Protokoll, um Details anzuzeigen.
4. Klicken Sie auf **Filter**, um nach der Protokolldatei zu suchen:
   a. Geben Sie die Suchkriterien an.
   b. Wählen Sie den Datumsbereich aus.
   c. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktualisieren**, um die Protokolldaten zu aktualisieren.
6. Klicken Sie auf **Vorherige** oder **Nächste**, um durch die Protokolldaten zu navigieren.

Warnungen

Sie können Alarmkriterien anpassen, indem sie vordefinierte Sicherheitsebenen für die Kategorisierung von Alarmen verwenden. Senden Sie Protokollereignisse an einen einzelnen oder mehrere E-Mail-Empfänger, indem Sie Alarme im Unternehmen oder in der Gruppe einrichten.

Hinweis

Informationen zu Nachrichten-IDs finden Sie unter *PolicyServer Nachrichten-IDs auf Seite B-1*.

PolicyServer Warnungen einrichten

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Wählen Sie eine Protokollereignisstufe aus:
   - Für Protokolle auf Unternehmensebene erweitern Sie **Unternehmen - Protokollereignisse**.
   - Für Protokolle auf Gruppenebene navigieren Sie zu **Gruppenname** > **Protokollereignisse.**

   Das Fenster "Protokoll" wird angezeigt. Alle Ereignisse der letzten sieben (7) Tage werden automatisch angezeigt.
3. Klicken Sie auf **Warnungen**.
4. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf eine freie Stelle, und wählen Sie **Hinzufügen**.

   Das Fenster **Warnung bearbeiten** wird angezeigt.
5. Geben Sie einen **Warnungsnamen** an.
6. Wählen Sie den Schweregrad von Protokollen aus, die Warnungen auslösen.

7. Wählen Sie die Nachrichten-IDs aus, die Warnungen auslösen.
8. Geben Sie eine E-Mail-Adresse pro Zeile ein. Diese E-Mail-Adresse erhalten eine Warnung in Form einer Benachrichtigung.
9. Wählen Sie aus, ob Warnungen basierend auf der Anzahl von Ereignissen während eines festgelegten Zeitraums gesendet werden sollen.
10. Klicken Sie auf **Fertig**.

PolicyServer zur Weiterleitung von SMS und E-Mail-Versand aktivieren

Diese Funktion kann nur auf PolicyServer unter Windows Server 2008 oder Windows Server 2008 R2 verwendet werden.

Prozedur

1. Melden Sie sich am Windows Server an.
2. Öffnen Sie **Servermanager**.
3. Navigieren Sie zu **Funktionen** > **Funktionen hinzufügen**.
4. Markieren Sie **SMTP-Server**.

   Das Fenster **Für SMTP-Server erforderliche Rollendienste und -funktionen hinzufügen** wird angezeigt.
5. Klicken Sie auf **Erforderliche Rollendienste hinzufügen**.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie erneut auf **Weiter**.
8. Klicken Sie auf **Installieren**.

   Die Webserver-IIS und der SMTP-Server werden installiert.
9. Klicken Sie auf **Schließen**.

10. Navigieren Sie zu **Start** > **Verwaltungstools** > **Internet Information Services (IIS) 6.0 Manager**.

    IIS 6.0 Manager wird geöffnet.

11. Erweitern Sie **Servername (lokales Gerät)**.

12. Klicken Sie mit der rechten Maustaste auf **[Virtueller SMTP-Server Nr. 1]** und klicken Sie auf **Eigenschaften**.

Hinweis

Markieren Sie zur künftigen Fehlerbehebung die Option **Protokollierung aktivieren**.

---

13. Navigieren Sie zu **Zugreifen** > **Verbindung...** und wählen Sie **Nur die folgende Liste** aus. Klicken Sie dann auf **Hinzufügen...**.

14. Geben Sie in das Feld **IP-Adresse** den Wert `127.0.0.1` ein, und klicken Sie anschließend auf **OK**.

Hinweis

Wiederholen Sie den Vorgang, um alle IP-Adressen auf dem lokalen Server anzugeben.

---

15. Klicken Sie auf **OK**.

16. Navigieren Sie zu **Übertragung** > **Erweitert...** und geben Sie die **Maskierte Domäne** in folgendem Format ein: `psproxy.<domain>.<com/org>`.

17. Klicken Sie zweimal auf **OK**, um das Fenster **Eigenschaften des virtuellen SMTP-Servers Nr. 1** zu schließen.

18. Navigieren Sie zu **Unternehmensrichtlinien** > **PolicyServer** > **PDA** > **E-Mail**.

19. Öffnen Sie **SMTP ServerName**, geben Sie `127.0.0.1` ein, und klicken Sie anschließend auf **Übernehmen**.

Erweiterten Standort konfigurieren

Erstellen Sie für optimale Ergebnisse einen SPF-DNS-Eintrag (Sender Policy Framework). Informationen zum Erstellen eines SPF-Datensatzes in anderen DNS-Servern (BIND) finden Sie in der Dokumentation des Herstellers.

Prozedur

1. Öffnen Sie **DNS-Management-Konsole** auf einem Windows DNS-Server.
2. Klicken Sie auf die Forward-Lookup-Zone für die Domäne, und wählen Sie **Andere neue Datensätze** aus.
3. Führen Sie einen Bildlauf nach unten durch und wählen Sie **TEXT (TXT)** aus.
4. Lassen Sie **Name des Datensatzes** leer und geben Sie Folgendes an:

   ```
   v=spf1 ip4:<IP-Adresse_des_externen_PolicyServer> -all
   ```

5. Klicken Sie auf **OK**.

Unternehmen - Berichte

PolicyServer zeichnet Protokollereignisse unter Verwendung vordefinierter Kriterien auf, wie z. B. Zugriffsversuche, Systemfehler, Änderungen an Benutzern oder Gruppen, Richtlinienänderungen sowie Probleme bei der Einhaltung von Richtlinien. Durch die Verwaltung von Protokollereignissen und Berichten können der Unternehmensadministrator und der Gruppenadministrator nach speziellen Protokollereignissen und Berichten über Server- und Client-Sicherheit suchen.Benutzer mit Unternehmensadministratorkonten können Berichte bei Bedarf oder zeitgesteuert generieren.

PolicyServer MMC verfügt über eine Vielzahl an integrierten Berichten, um den Status der Endpoint Encryption Geräteverschlüsselung, die Aktivität von Endpoint Encryption Benutzern oder Geräten und die PolicyServer Integrität zu überprüfen.

Hinweis

Nur der Administrator des Unternehmens kann Berichte verwenden.

Berichtoptionen

In der folgenden Tabelle werden die für die verschiedenen Berichte verfügbaren Optionen beschrieben. Klicken Sie mit der rechten Maustaste auf einen Bericht, um die verfügbaren Optionen anzuzeigen.

Berichtoptionen	Beschreibung
Löschen	Entfernt alle im Ergebnisfenster angezeigten Informationen, löscht diese aber nicht.
Fehler anzeigen	Zeigt eine Beschreibung des Fehlers an, der dazu geführt hat, dass der Bericht ungültig ist.
Bericht anzeigen	Zeigt den Bericht an.
Nächste Seite	Wechseln Sie zur nächsten Seite der Suchelemente.
Vorherige Seite	Wechseln Sie zur vorherigen Seite der Suchelemente.
Aktualisieren	Aktualisieren Sie den Status eines übermittelten Berichts.
Bericht entfernen	Löscht den Bericht.
Bericht planen	Konfigurieren Sie einen Zeitplan für den Bericht zur Ausführung an einem bestimmten Tag oder zu einer bestimmten Uhrzeit.
Bericht übermitteln	Generieren Sie den ausgewählten Bericht.

Berichtssymbole

In der folgenden Tabelle werden die Symbole beschrieben, die neben einem Bericht angezeigt werden.

Symbol	Beschreibung
	Standardberichte können je nach Bedarf übermittelt werden, um Statistiken und andere Nutzungsmetriken anzuzeigen.
	Alarmberichte informieren Unternehmensadministratorkonten über potenzielle Sicherheitsprobleme.

Berichttypen

Berichte erleichtern das Verständnis von Protokollinformationen. PolicyServer MMC unterteilt Berichte in zwei gesonderte Kategorien:

- **Standardberichte**: Spezielle Protokollinformationen werden in Standardberichten in einem Berichtsformat erfasst. Sie können Standardberichte je nach Bedarf übermitteln.
- **Alarmberichte**: Alarmberichte senden eine Warnung an den Administrator im Unternehmen und erfassen den Sicherheitsvorfall in einem Bericht.

Hinweis

Nur der Administrator des Unternehmens kann Berichte verwenden.

Standardberichte

Die folgende Tabelle ermittelt ein Verständnis darüber, welche Standardberichte bei Bedarf erstellt werden können.

TABELLE 16-1. Liste mit Standardberichten

BERICHTNAME	BESCHREIBUNG
Geräteverschlüsselungsstatus	Listet den Verschlüsselungsstatus für alle Endpoint Encryption Geräte in einem Unternehmen in einem Bericht auf.
Gerätebetriebssysteme und Anzahl	Meldet alle Gerätebetriebssysteme und die Anzahl für jedes System.
Geräteversion und Anzahl	Meldet alle Versionen der Endpoint Encryption Geräte und die Anzahl für jede Version.
Geräte nach letztem Synchronisierungsdatum	Meldet alle Endpoint Encryption Geräte, die in den letzten x Tagen mit dem PolicyServer synchronisiert wurden.
Nicht kommunizierende Geräte	Meldet die Endpoint Encryption Geräte, die seit <X> Tagen nicht mit PolicyServer kommuniziert haben.
Geräte mit zuletzt angemeldetem Benutzer	Meldet alle Endpoint Encryption Geräte und den letzten Benutzer, der sich authentifiziert hat.
Verfügbare Unternehmenslizenzen	Meldet die in der Lizenz verbleibenden Tage, verfügbare Endpoint Encryption Geräte und Benutzer sowie die Anzahl der genutzten Geräte und Benutzer.
Unternehmen - Inaktive Benutzer	Meldet alle Endpoint Encryption Benutzer, die sich während eines angegebenen Zeitraums nicht bei einem der Endpoint Encryption Geräte angemeldet haben.
Benutzeraktivität im Unternehmen	Meldet die Gesamtzahl der Endpoint Encryption Geräte, die Gesamtzahl der Endpoint Encryption Benutzer und die Anzahl der PolicyServer MMC Benutzer sowie die Endpoint Encryption Geräteaktivität.
Nicht vollständig verschlüsselte Full Disk Encryption Geräte	Meldet alle Endpoint Encryption Geräte in den letzten <X> Tagen, die mit der Verschlüsselung begonnen, diese aber nicht abgeschlossen haben.

BERICHTNAME	BESCHREIBUNG
Benutzeraktivität nach Tag	Meldet die Endpoint Encryption Benutzeraktivität innerhalb von <X> Tagen für den angegebenen Benutzer.
Hinzugefügte Benutzer	Meldet alle Endpoint Encryption Benutzer, die in den letzten <X> Tagen hinzugefügt wurden.
Benutzer, die sich nie an einem Gerät angemeldet haben	Meldet alle Endpoint Encryption Benutzer, die sich niemals bei einem Endpoint Encryption Gerät authentifiziert haben.

Ausführen von Standardberichten

Spezielle Protokollinformationen werden in Standardberichten in einem Berichtsformat erfasst. Sie können Standardberichte je nach Bedarf übermitteln.

Prozedur

1. Klicken Sie auf den gewünschten Bericht, und wählen Sie anschließend **Bericht übermitteln** aus.
2. Geben Sie die Berichtsparameter an (falls erforderlich), und klicken Sie auf **Übernehmen**.

   Der Bericht wird angezeigt.
3. Um den Bericht anzuzeigen, navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.

Alarmberichte

Die Angaben in der folgenden Tabelle vermitteln ein Verständnis dafür, wann PolicyServer Alarmberichte generiert.

ALARMNAME	BESCHREIBUNG
Aufeinanderfolgende fehlgeschlagene Anmeldeversuche auf einem einzelnen Gerät	Es wird eine Warnung gesendet, wenn mehrere aufeinanderfolgende Authentifizierungsversuche bei einem beliebigen Endpoint Encryption Gerät fehlgeschlagen sind.
Warnung zur Protokollintegrität	Es wird eine Warnung gesendet, wenn es Anhaltspunkte dafür gibt, dass die PolicyServer Protokolle manipuliert wurden.
Warnung bei Manipulation an Richtlinien	Es wird eine Warnung gesendet, wenn PolicyServer erkennt, dass Richtlinien manipuliert wurden.
Durchgesetzte primäre und sekundäre Aktion	Es wird eine Warnung gesendet, wenn PolicyServer nicht verbunden ist und die primäre oder sekundäre Aktion durchgesetzt wurde.

Ausführen von Alarmberichten

Um den generierten Bericht anzuzeigen, navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf den gewünschten Alarmbericht, und wählen Sie anschließend **Warnungen konfigurieren**.

   Das Fenster **Warnungskonfiguration** wird angezeigt.

2. Geben Sie die **SMTP-Server-Adresse** und den **Absender** für die ausgehenden E-Mail-Nachrichten an.

3. Klicken Sie auf **Übernehmen**.

4. Klicken Sie auf den gewünschten Bericht, und wählen Sie **Warnung übermitteln** aus.

Anzeigen von Berichten

Hinweis

Nur der Administrator des Unternehmens kann Berichte verwenden.

Prozedur

1. Navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.
2. Klicken Sie auf den gewünschten Bericht, und wählen Sie dann **Bericht anzeigen** aus.

   Der Bericht wird angezeigt.
3. Um den Bericht zu exportieren, klicken Sie auf das Symbol **Speichern**, und wählen Sie anschließend **Excel** oder **Acrobat (PDF)-Datei** aus.

Zeitgesteuerte Berichte

Zeitplan erstellen, um einen Bericht an einem bestimmten Datum zu einer bestimmten Uhrzeit automatisch auszuführen.

Prozedur

1. Öffnen Sie **Unternehmen - Berichte**.
2. Klicken Sie auf den gewünschten Bericht, und wählen Sie anschließend **Bericht planen** aus.

   Das Fenster **Berichtsparameter** wird angezeigt.
3. Geben Sie die Berichtsparameter an, und klicken Sie anschließend auf **Übernehmen**.

   Das Fenster **Berichtsplanung** wird angezeigt.

4. Geben Sie das Berichtsintervall sowie das Datum und die Uhrzeit an, und klicken Sie auf **Übernehmen**.

   Der zeitgesteuerte Bericht wurde geplant.

5. Um die zeitgesteuerten Berichte anzuzeigen, navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Zeitgesteuerte Berichte**.

Anzeigen von Berichtsfehlern

Es kann vorkommen, dass ein Bericht aufgrund eines Fehlers nicht ordnungsgemäß ausgeführt wird. Informationen zur Anzeige von PolicyServer Nachrichten-IDs finden Sie unter *PolicyServer Nachrichten-IDs auf Seite B-1*.

Prozedur

1. Navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.

2. Klicken Sie mit der rechten Maustaste auf den Bericht mit einem Fehler, und wählen Sie dann **Fehler anzeigen** aus.

   Die Berichtsfehlermeldung wird angezeigt.

Kapitel 17

Wartung und technischer Support

In den folgenden Themen wird der Wartungsvertrag erläutert und beschrieben, wie Sie online nach Lösungen suchen, das Support-Portal verwenden, mit Trend Micro Kontakt aufnehmen und zusätzliche Ressourcen finden.

Es werden folgende Themen behandelt:

- *Wartungsvertrag auf Seite 17-2*
- *Ressourcen zur Fehlerbehebung auf Seite 17-6*
- *Kontaktaufnahme mit Trend Micro auf Seite 17-8*
- *Andere Ressourcen auf Seite 17-9*

Wartungsvertrag

Ein Wartungsvertrag zwischen Ihrem Unternehmen und Trend Micro regelt, in welchem Umfang Sie nach Zahlung der entsprechenden Gebühren Anrecht auf den Erhalt von technischem Support und Produkt-Updates haben. Beim Kauf eines Trend Micro Produkts enthält die Lizenzvereinbarung, die Sie mit dem Produkt erhalten, die Bestimmungen des Wartungsvertrags für dieses Produkt.

Eine Lizenz für die Trend Micro Software enthält üblicherweise das Recht auf Produkt- und Pattern-Datei-Updates und grundlegenden technischen Support (Wartung) für ein (1) Jahr ab Kaufdatum. Nach Ablauf dieser Frist muss der Wartungsvertrag jährlich zu den jeweils aktuellen Wartungsgebühren von Trend Micro verlängert werden.

Auch nach Ablauf des Wartungsvertrags kann eine Virensuche durchgeführt werden. Allerdings können Sie das Produkt nicht mehr aktualisieren, auch nicht manuell. Ebenso haben Sie keinen Anspruch mehr auf technischen Support von Trend Micro.

Normalerweise werden Sie neunzig (90) Tage vor Ablauf des Wartungsvertrags darauf hingewiesen, dass der Vertrag in Kürze abläuft. Sie können den Wartungsvertrag aktualisieren, indem Sie eine Verlängerung erwerben. Dies ist über Ihren Händler, den Trend Micro Vertrieb oder den Trend Micro Online-Registrierungsserver möglich. Sie erreichen ihn unter folgendem URL:

Online-Registrierungssystem

Den Wartungsvertrag verlängern

Trend Micro oder dazu autorisierte Händler bieten allen registrierten Benutzern technischen Support, Downloads und Programm-Updates für die Dauer eines (1) Jahres. Nach Ablauf dieser Frist muss der Wartungsvertrag verlängert werden.

Nach Ablauf des Wartungsvertrags sind grundlegende Operationen weiter verfügbar. Sie können jedoch keine neuen Benutzer und Geräte zu PolicyServer hinzufügen, weder über PolicyServer MMC, über Agent-Installationen noch über Control Manager. Daher sollte der Wartungsvertrag sobald wie möglich verlängert werden.

Wenn Kunden ein Upgrade durchführen, wird die vorhandene Lizenz bis zum Ablauf akzeptiert.

Prozedur

1. Gehen Sie wie folgt vor, um den Wartungsvertrag zu verlängern:

   - Wenden Sie sich an den Händler, bei dem Sie auch das Produkt erworben haben. Die Verlängerung des Wartungsvertrags um ein weiteres Jahr wird per Post an den Hauptansprechpartner für Registrierungsfragen gesendet.
   - Melden Sie sich auf der Trend Micro Website für die Online-Registrierung an, um die Registrierungsdaten Ihres Unternehmens anzuzeigen oder zu ändern: https://olr.trendmicro.com/registration/

2. Um die Registrierungsdaten anzuzeigen, geben Sie die Anmelde-ID und das Kennwort an, die Sie bei der ersten Registrierung des Produkts bei Trend Micro (als Neukunde) erstellt haben, und klicken Sie anschließend auf **Anmelden**.

3. Informationen zur Aktualisierung der Umgebung mit dem neuen Aktivierungscode finden Sie unter *Neue Produktlizenz aktivieren auf Seite 17-3*.

Testlizenz

Sie können Endpoint Encryption für einen zeitlich begrenzten Testzeitraum von 30 Tagen installieren und bewerten. Während der Installation von PolicyServer werden die Unternehmensdatenbank und das Unternehmensadministratorkonto angelegt. PolicyServer funktioniert normal mit allen Client-Anwendungen, einer unbegrenzten Zahl von Geräten und bis zu 100 Benutzern für einen Testzeitraum von 30 Tagen. Wenden Sie sich nach 30 Tagen an den Technischen Support von Trend Micro, um eine Lizenzdatei zu erhalten. Nach Ablauf des Testzeitraums funktionieren Endpoint Encryption Benutzerkonten und Geräte normal.

Neue Produktlizenz aktivieren

Eine kostenfreie Testlizenz für 30 Tage ist verfügbar, um Endpoint Encryption zu installieren und zu bewerten. Wenn Sie von der Testlizenz aus auf eine Produktlizenz umsteigen, stellen Sie sicher, dass Sie vor Ablauf der Lizenz das Upgrade auf die Vollversion durchführen.

Prozedur

1. Melden Sie sich bei dem Server an, auf dem PolicyServer momentan installiert ist.
2. Navigieren Sie zu dem Ordner, der die Programmdateien von PolicyServer enthält, und öffnen Sie den Ordner `Tools`.
3. Führen Sie `TMEE_License_Renewal.exe` aus.

   Das **Tool zur Lizenzverlängerung** wird geöffnet.
4. Klicken Sie unter **Lizenz verlängern** auf **Online verlängern**, um auf die Registrierungs-Website von Trend Micro zuzugreifen.

   Nach Abschluss der Registrierung erhalten Sie von Trend Micro eine E-Mail mit dem Aktivierungscode.
5. Geben Sie den neuen Aktivierungscode für das Produkt ein.
6. Klicken Sie auf **Aktivieren**.
7. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**, um fortzufahren.
8. Klicken Sie auf **Beenden**.

Die aktualisierte Endpoint Encryption Produktlizenz ist sofort verfügbar.

Produktlizenz anzeigen

Sie können mit PolicyServer MMC den aktuellen Status der Lizenz anzeigen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Klicken Sie mit der rechten Maustaste auf das Unternehmen, und wählen Sie **Aktivierung/Lizenz**.

   Das Fenster **Registrierungsinformationen** wird angezeigt.
3. Überprüfen Sie die folgenden Optionen.

Option	Bezeichnung
Aktivierungscode	Bei einer Vollversion wird der Aktivierungscode angezeigt. Bei anderen Lizenztypen wird der Name der Lizenz angezeigt.
Anfangsdatum	Das Datum, an dem die Lizenz aktiviert wurde.
Ablaufdatum	Das Datum, an dem die Lizenz verlängert werden muss. Nach dem Ablauf einer Lizenz können vorhandene Endpoint Encryption Benutzer sich weiterhin bei Endpoint Encryption Geräten anmelden, jedoch können keine neuen Endpoint Encryption Geräte oder Benutzer dem Unternehmen hinzugefügt werden.
Anzahl der Geräte	Die laut der Lizenz zulässige Anzahl der Endpoint Encryption Geräte.
Anzahl der installierten Geräte	Die im Unternehmen momentan konfigurierte Anzahl der Endpoint Encryption Geräte.
Anzahl der Benutzer	Die laut der Lizenz zulässige Gesamtzahl der Endpoint Encryption Benutzer.
Anzahl der erstellten Benutzer	Die dem Unternehmen momentan hinzugefügte Anzahl an Endpoint Encryption Benutzern.
Aktivierungszeitraum in Tagen	Die Anzahl der verbleibenden Tage bis zum Ablauf der Lizenz.

4. Klicken Sie auf **Schließen**.

Produktwartung

Von Zeit zu Zeit wird Trend Micro möglicherweise einen Patch für ein gemeldetes bekanntes Problem oder ein Upgrade für das Produkt veröffentlichen. Wenn Sie herausfinden möchten, ob Patches verfügbar sind, besuchen Sie: http://downloadcenter.trendmicro.com/?regs=DE

Patches sind mit einem Datum versehen. Falls Patches vorliegen, öffnen Sie die Readme-Datei, um festzustellen, ob der Patch anwendbar ist. Falls ja, befolgen Sie die Upgrade-Anweisungen in der Readme-Datei.

Ressourcen zur Fehlerbehebung

Bevor Sie mit dem technischen Support Kontakt aufnehmen, sollten Sie die folgenden Online-Ressourcen von Trend Micro besuchen:

Trend Community

Um Hilfe zu erhalten, Erfahrungen auszutauschen, Fragen zu stellen und Sicherheitsprobleme mit anderen Benutzern, Enthusiasten und Sicherheitsexperten zu diskutieren, navigieren Sie zu:

http://community.trendmicro.com/

Das Support-Portal verwenden

Beim Trend Micro Support Portal handelt es sich um eine Online-Ressource mit brandaktuellen Informationen über häufige und ungewöhnliche Probleme, auf die Sie rund um die Uhr zugreifen können.

Prozedur

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie ein Produkt oder einen Dienst aus dem entsprechenden Listenfeld aus, und geben Sie weitere verwandte Informationen an, wenn Sie dazu aufgefordert werden.

   Die Produktseite **Technischer Support** wird angezeigt.
3. Suchen Sie über das Feld **Support durchsuchen** nach verfügbaren Lösungen.

4. Wenn keine Lösung gefunden wird, klicken Sie in der linken Navigationsleiste auf **Submit a Support Case**, und fügen Sie relevante Details hinzu, oder übermitteln Sie den Support-Fall hier:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   Ein Trend Micro Support-Ingenieur untersucht den Fall und antwortet innerhalb von 24 Stunden oder schneller.

Security Intelligence Community

Die Cybersecurity-Experten von Trend Micro sind ein Eliteteam im Bereich Security Intelligence, das sich auf Erkennung und Analyse von Bedrohungen, Sicherheit in Cloud- und virtualisierten Umgebungen sowie Datenverschlüsselung spezialisiert hat.

Navigieren Sie zu http://www.trendmicro.de/sicherheitsinformationen/index.html. Sie finden dort Informationen über:

- Trend Micro Blogs, Twitter, Facebook, YouTube und andere soziale Medien
- Bedrohungsberichte, Forschungsarbeiten und Spotlight-Artikel
- Lösungen, Podcasts und Newsletter von globalen Insidern aus der Sicherheitsbranche
- Kostenlose Tools, Apps und Widgets.

Bedrohungsenzyklopädie

Die meiste Malware besteht aus "kombinierten Bedrohungen", d. h., mindestens zwei Technologien wurden kombiniert, um die Sicherheitsprotokolle des Computers zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie schaffen. Die Bedrohungsenzyklopädie stellt eine umfangreiche Liste aus Namen und Symptomen für verschiedene kombinierte Bedrohungen bereit, einschließlich bekannter Malware, Spam, bösartiger URLs und bekannter Schwachstellen.

Navigieren Sie zu http://www.trendmicro.com/vinfo/de/virusencyclo/default.asp. Sie finden dort weitere Informationen über:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv oder im Umlauf sind
- Zusammenhängende Seite mit Bedrohungsinformationen, die ein vollständiges Bild der Webangriffe zeichnen
- Beratung zu Internet-Bedrohungen über gezielte Angriffe und Sicherheitsbedrohungen
- Informationen zu Webangriffen und Online-Trends
- Wöchentliche Malware-Berichte.

Kontaktaufnahme mit Trend Micro

Trend Micro Mitarbeiter sind per Telefon, Fax oder E-Mail verfügbar:

Adresse	Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.	+49 (0) 811 88990-700
Fax	+4981188990799
Internet-Adresse	http://www.trendmicro.de/
E-Mail	support@trendmicro.com

- Weltweite Support-Büros:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

  http://docs.trendmicro.com/de-de/home.aspx

Problemlösung beschleunigen

Um das Lösen eines Problems zu verbessern, halten Sie die folgenden Informationen bereit:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zu Gerät oder Netzwerk
- Marke und Modell des Computers sowie weitere, an den Endpunkt angeschlossene Hardware
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Version und Service Pack des verwendeten Betriebssystems
- Endpunkt-Clientversion
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

Andere Ressourcen

Neben den Lösungen und dem Support sind online viele andere hilfreiche Ressourcen verfügbar, die Ihnen helfen, auf dem Laufenden zu bleiben, über Innovationen informiert zu werden und Informationen über aktuelle Sicherheitsbedrohungen zu erhalten.

TrendEdge

Sie können nach Informationen über nicht unterstützte, innovative Techniken, Tools und bewährte Methoden für Produkte und Dienste von Trend Micro suchen. Die TrendEdge Datenbank enthält zahlreiche Dokumente zu vielen verschiedenen Themen für Partner, Mitarbeiter oder andere interessierte Parteien von Trend Micro.

Die neuesten Informationen, die in TrendEdge aufgenommen wurden, finden Sie unter:

http://trendedge.trendmicro.com/

Download Center

Von Zeit zu Zeit wird Trend Micro möglicherweise einen Patch für ein gemeldetes bekanntes Problem oder ein Upgrade für ein bestimmtes Produkt oder einen bestimmten Dienst veröffentlichen. Wenn Sie herausfinden möchten, ob Patches verfügbar sind, besuchen Sie:

http://downloadcenter.trendmicro.com/?regs=DE

Wenn ein Patch noch nicht angewendet wurde (Patches sind mit Datumsangaben versehen), öffnen Sie die Readme-Datei, um festzustellen, ob der Patch für Ihre Umgebung von Bedeutung ist. In der Readme-Datei finden Sie auch die Installationsanweisungen.

TrendLabs

TrendLabs℠ ist ein weltweites Netzwerk aus Forschungs-, Entwicklungs- und Lösungszentren, das rund um die Uhr Bedrohungen überwacht, Präventionsstrategien entwickelt sowie rasche und kontinuierliche Lösungen bereitstellt. TrendLabs bildet die Grundlage der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslage und liefert wirksame Sicherheitsmaßnahmen für die Erkennung, Vermeidung und Beseitigung von Angriffen. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen über TrendLabs finden Sie unter:

http://www.trendmicro.de/newsroom/faces/index.html

Anhänge

Anhänge

Anhang A

Einführung in Trend Micro™ Control Manager™

Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Administratoren können mit den Funktionen zur Richtlinienverwaltung die Produkteinstellungen für die verwalteten Produkte und Endpunkte konfigurieren und verteilen. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für die Verwaltung der Produkte und Dienste für Virenschutz und Content Security im gesamten Netzwerk.

Mit Control Manager kann der Systemadministrator Aktivitäten wie beispielsweise auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Viren-/Malware-Eintrittsstellen überwachen und aufzeichnen. Der Systemadministrator kann Update-Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Zu den Beispielen für Update-Komponenten zählen die Viren-Pattern-Dateien, die Scan Engine und die Anti-Spam-Regeln. Mit Control Manager sind sowohl manuelle als auch zeitgesteuerte Updates möglich. Mit Control Manager können Produkte in Gruppen oder einzeln konfiguriert und verwaltet werden.

Dieses Kapitel umfasst die folgenden Themen:

- *Control Manager Standard und Advanced auf Seite A-3*
- *Einführung in die Funktionen von Control Manager auf Seite A-3*
- *Control Manager Architektur auf Seite 3-3*

- *Endpoint Encryption bei Control Manager registrieren auf Seite A-8*
- *Grundlegendes zum Benutzerzugriff auf Seite A-9*
- *Grundlegendes zum Produktverzeichnis auf Seite A-17*
- *Neue Komponenten herunterladen und verteilen auf Seite A-41*
- *Protokolle verwenden auf Seite A-70*
- *Grundlegendes zu Berichten auf Seite A-74*

Control Manager Standard und Advanced

Control Manager ist in zwei Versionen erhältlich: Standard und Advanced. Control Manager Advanced enthält Funktionen, die in Control Manager Standard nicht enthalten sind. Beispielsweise unterstützt Control Manager Advanced eine übersichtlich gegliederte Verwaltungsstruktur. Das bedeutet, das Control Manager Netzwerk kann von einem übergeordneten Control Manager Advanced Server verwaltet werden, wobei mehrere untergeordnete Control Manager Advanced Server Meldungen an den übergeordneten Control Manager Advanced Server senden. Der übergeordnete Server erfüllt die Aufgaben eines Knotenpunkts für das gesamte Netzwerk.

Hinweis

Control Manager Advanced unterstützt die folgenden untergeordneten Control Manager Server:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard Server werden als untergeordnete Server nicht unterstützt.

Eine vollständige Liste aller Funktionen der Standard- und Advanced-Versionen von Control Manager Server finden Sie in der *Trend Micro Control Manager* Dokumentation.

Einführung in die Funktionen von Control Manager

Control Manager wurde von Trend Micro zur Verwaltung von Antiviren- und Content-Security-Produkten und Diensten entwickelt, die in den LANs und WANs eines Unternehmens eingesetzt werden.

TABELLE A-1. Control Manager Funktionen

FUNKTION	BESCHREIBUNG
Richtlinienverwaltung	Systemadministratoren können von einer einzelnen Management-Konsole aus mit Hilfe von Richtlinien Produkteinstellungen für verwaltete Produkte und Endpunkte konfigurieren und verteilen.
Zentrale Konfiguration	Mit dem Produktverzeichnis und einer übersichtlich gegliederten Verwaltungsstruktur können Sie mit Hilfe dieser Funktionen Reaktionen auf Viren und Content-Security-Aufgaben von einer einzelnen Management-Konsole aus koordinieren. Diese Funktionen tragen dazu bei, die einheitliche Durchsetzung der Viren/Malware- und Content-Security-Richtlinien in Ihrem Unternehmen sicherzustellen.
Proaktive Ausbruchsprävention	Mit den Outbreak Prevention Services (OPS) schützen Sie Ihr Netzwerk proaktiv vor einem bevorstehenden Viren-/Malware-Ausbruch.
Sichere Kommunikationsinfrastruktur	Die Kommunuikationsinfrastruktur des Control Managers basiert auf dem Secure Socket Layer (SSL) Protokoll. Je nach gewählter Sicherheitseinstellung kann der Control Manager Nachrichten mit oder ohne Authentifizierung verschlüsseln.
Sichere Konfiguration und sicherer Komponenten-Download	Mit diesen Funktionen können Sie einen sicheren Zugriff auf die Webkonsole und einen sicheren Komponenten-Download konfigurieren.
Aufgabenverteilung	Der Systemadministrator kann den Benutzern der Webkonsole von Control Manager personalisierte Konten mit benutzerdefinierten Berechtigungen einrichten. In den Benutzerkonten ist festgelegt, was der Benutzer in einem Control Manager Netzwerk sehen und welche Aktionen er durchführen kann. Die Nutzung der Konten kann über Benutzerprotokolle nachverfolgt werden.

FUNKTION	BESCHREIBUNG
Befehlsverfolgung	Mit dieser Funktion können Sie alle Befehle überwachen, die auf der Webkonsole von Control Manager ausgeführt werden. Das Rückverfolgen von Befehlen ist eine nützliche Option zur Überprüfung, ob Control Manager lang andauernde Befehle erfolgreich ausgeführt hat, wie z. B. das Update und die Verteilung von Viren-Pattern.
Manuelle Produktsteuerung	Verwaltete Produkte in Echtzeit steuern. Control Manager sendet Konfigurationsänderungen, die über die Webkonsole durchgeführt wurden, umgehend an die verwalteten Produkte. Systemadministratoren können manuelle Suchen über die Webkonsole ausführen. Dieses Befehlssystem ist bei einem Viren-/Malware-Ausbruch unverzichtbar.
Zentrale Update-Steuerung	Aktualisiert Viren-Pattern, Anti-Spam-Regeln, Scan Engines und andere Antiviren- oder Content-Security-Komponenten, die dazu beitragen, dass alle verwalteten Produkte aktuell sind.
Zentrale Berichterstellung	Gibt einen Überblick über die Leistung der Antiviren- und Content-Security-Produkte mit Hilfe von umfangreichen Protokollen und Berichten. Control Manager erfasst die Protokolle von allen verwalteten Produkten, d. h., Sie müssen nicht mehr die Protokolle der jeweiligen einzelnen Produkte überprüfen.

Control Manager Architektur

Trend Micro Control Manager bietet Funktionen, um Produkte und Dienste von Trend Micro von einer zentralen Stelle aus zu steuern. Diese Anwendung vereinfacht die Verwaltung der Viren/Malware- und Content-Sicherheitsrichtlinien im Unternehmen. Die folgende Tabelle enthält eine Liste der Komponenten, die von Control Manager verwendet werden.

TABELLE A-2. Control Manager Komponenten

KOMPONENTE	BESCHREIBUNG
Control Manager server	Dient als ein Repository für alle Daten, die von den Agents erfasst werden. Dabei kann es sich um Server der Standard Edition oder der Advanced Edition handeln. Ein Control Manager Server unterstützt die folgenden Funktionen: • Eine SQL-Datenbank, in der die Konfigurationen und die Protokolle der verwalteten Produkte gespeichert werden. Control Manager arbeitet mit der Datenbank Microsoft SQL Server (`db_ControlManager.mdf`) zusammen, um Daten zu speichern, die in Protokollen, Communicator Zeitplänen, verwalteten Produkten und Informationen zu untergeordneten Servern, Benutzerkonten, Netzwerkumgebungen und Benachrichtigungseinstellungen enthalten sind. • Ein Webserver als Host für die Webkonsole von Control Manager. • Ein Mail-Server, der die Benachrichtigungen bei Ereignissen in Form von E-Mail-Nachrichten versendet. Control Manager kann Benachrichtigungen an Einzelpersonen oder Empfängergruppen über Ereignisse senden, die im Control Manager Netzwerk auftreten. In Event Center können Sie konfigurieren, ob Benachrichtigungen als E-Mail-Nachrichten, Windows Ereignisprotokoll, MSN Messenger, SNMP, Syslog, Pager oder an eine andere interne oder dem Branchenstandard entsprechende Anwendung gesendet werden, die von Ihrem Unternehmen zur Versendung von Benachrichtigungen eingesetzt wird. • Ein Berichtserver, der nur zum Umfang der Advanced Edition gehört, generiert Berichte zu Antiviren- und Content-Sicherheitsprodukten. Ein Control Manager Bericht ist eine Online-Sammlung von Zahlen über das Auftreten von Ereignissen zu Sicherheitsbedrohungen und Content-Sicherheit im Control Manager Netzwerk, die ein Sicherheitsrisiko darstellen.

KOMPONENTE	BESCHREIBUNG
Das Trend Micro Management Communication Protocol	MCP verarbeitet die Interaktion von Control Manager Server mit den verwalteten Produkten, die den Agent der nächsten Generation unterstützen. MCP ist das neue Rückgrat für das Control Manager System. MCP Agents werden mit den verwalteten Produkten installiert und nutzen eine Ein-Weg- oder Zwei-Wege-Kommunikation zur Kommunikation mit Control Manager. MCP Agents rufen Anweisungen und Updates vom Control Manager ab.
Trend Micro Management Infrastructure	Verarbeitet die Interaktion von Control Manager Server mit älteren verwalteten Produkten. Der Communicator bzw. das Message Routing Framework ist das Kommunikationsrückgrat für das ältere Control Manager System. Dabei handelt es sich um eine Komponente der Trend Micro Management Infrastructure (TMI). Communicators verarbeiten die gesamte Kommunikation zwischen dem Control Manager Server und den älteren verwalteten Produkten. Die Kommunikation mit den älteren verwalteten Produkten erfolgt durch Interaktion mit Control Manager 2.x Agents.
Control Manager 2.x Agents	Empfangen Befehle von Control Manager Server und senden Statusinformationen und Protokolle an den Control Manager Server Beim Control Manager Agent handelt es sich um eine Anwendung, die auf dem Server eines verwalteten Produkts installiert ist und die es möglich macht, dass Control Manager das Produkt verwaltet. Agents interagieren mit dem verwalteten Produkt und Communicator. Ein Agent dient als Brücke zwischen dem verwalteten Produkt und Communicator. Aus diesem Grund sollten Sie alle Agents auf demselben Computer wie die verwalteten Produkte installieren.

KOMPONENTE	BESCHREIBUNG
Webbasierte Management-Konsole	Ermöglicht, dass ein Administrator Control Manager von quasi jedem Computer mit einer Internet-Verbindung und Windows™ Internet Explorer™ aus verwaltet. Bei der Management-Konsole von Control Manager handelt es sich um eine Web-basierte Konsole, die im Internet über den Microsoft Internet Information Server (IIS) veröffentlicht wurde und die vom Control Manager Server gehostet wird. Mit dieser Lösung können Sie das Control Manager Netzwerk von einem beliebigen Computer verwalten, auf dem ein kompatibler Webbrowser verwendet wird.
Widget-Framework	Ermöglicht Administratoren, ein angepasstes Dashboard zur Überwachung des Control Manager Netzwerks zu erstellen.

Endpoint Encryption bei Control Manager registrieren

Sie können den Endpoint Encryption Server erst bei einem Control Manager Server registrieren, nachdem Sie sichergestellt haben, dass der Server und der Control Manager Server zum selben Netzwerksegment gehören.

Prozedur

1. Klicken Sie auf **Administration** > **Control Manager Settings**.

   Hinweis

   Control Manager verwendet den Namen, den Sie im Feld "Host-Name" angegeben haben, um den Endpoint Encryption Server zu identifizieren. Der Host-Name wird im Produktverzeichnis von Control Manager angezeigt.

   Das Fenster **Control Manager Settings** wird angezeigt.

2. Geben Sie unter **Connection settings** den Namen des Endpoint Encryption Servers in das Feld **Entity display name** ein.

3. Legen Sie unter **Control Manager Server Settings** die folgenden Einstellungen fest:

   a. Geben Sie den Host-Namen oder die IP-Adresse des Control Manager Servers in das Eingabefeld "Server-FQDN" oder "IP-Adresse" ein.

   b. Geben Sie die Portnummer des MCP Agents ein, der für die Kommunikation mit Control Manager verantwortlich ist.

   c. Wenn Sie für die Sicherheit von Control Manager "Mittel" festgelegt haben (Kommunikation über HTTPS und HTTP ist zulässig zwischen Control Manager und dem MCP Agent der verwalteten Produkte), wählen Sie **Connect through HTTPS**.

   d. Wenn Ihr Netzwerk eine Authentifizierung erfordert, geben Sie den Benutzernamen und das Kennwort des IIS-Servers in die Felder **Username** und **Password** ein.

   e. Wenn Sie ein NAT-Gerät einsetzen, wählen Sie **Enable two-way communication port forwarding**, und geben Sie die IP-Adresse und Portnummer des NAT-Geräts in die Felder **IP address** und **port number** ein.

   Weitere Informationen zur Verwaltung von Produkten in Control Manager finden Sie im *Administratorhandbuch für Trend Micro Control Manager*.

4. Klicken Sie auf der Management-Konsole von Control Manager auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

5. Der Endpoint Encryption Server wird im Produktverzeichnis angezeigt.

Grundlegendes zum Benutzerzugriff

Die Zugriffskontrolle von Control Manager besteht aus den folgenden vier Abschnitten.

TABELLE A-3. Optionen für den Control Manager Benutzerzugriff

ABSCHNITT	BESCHREIBUNG
Mein Konto	Das Fenster **My Account** enthält die Kontodaten, über die Control Manager für einen bestimmten Benutzer verfügt. Die Informationen im Fenster **My Account** sind vom Benutzer abhängig.
Benutzerkonten	Im Fenster **User Accounts** werden alle Benutzer von Control Manager angezeigt. Das Fenster enthält ebenfalls Optionen für Benutzer, die Control Manager Benutzerkonten erstellen und pflegen möchten. Mit Hilfe dieser Funktionen definieren Sie klare Verantwortungsbereiche für Benutzer, indem Sie die Zugriffsrechte auf bestimmte verwaltete Produkte einschränken und begrenzen, welche Aktionen Benutzer auf den verwalteten Produkten ausführen können. Diese Funktionen sind: • Ausführen • Konfigurieren • Verzeichnis bearbeiten
Benutzerrollen	Im Fenster **User Roles** werden alle Benutzerrollen von Control Manager angezeigt. Das Fenster enthält ebenfalls Optionen für Benutzer, die Control Manager Benutzerrollen erstellen und pflegen möchten. Mit Benutzerrollen wird definiert, auf welche Bereiche der Webkonsole von Control Manager ein Benutzer Zugriff hat.

ABSCHNITT	BESCHREIBUNG
Benutzergruppen	Im Fenster **User Groups** befinden sich die Control Manager Gruppen sowie Optionen zum Erstellen von Gruppen. Control Manager verwendet Gruppen als einfache Methode, um Benachrichtigungen an mehrere Benutzer zu senden, ohne dass dazu die Benutzer einzeln ausgewählt werden müssten. Control Manager lässt es nicht zu, dass Administratoren eine Gruppe mit denselben Zugriffsrechten wie eine andere Gruppe erstellen.

Hinweis

Sie können Benutzern verschiedene Zugriffsrechte und Berechtigungen zuweisen, um bestimmte Verwaltungsaufgaben zu delegieren, ohne dazu die Sicherheit zu beeinträchtigen.

Control Manager Benutzerzugriff mit Endpoint Encryption Benutzerzugriff

Der Benutzerzugriff von Endpoint Encryption entspricht dem Benutzerzugriff von Control Manager. Administratoren können festlegen, auf welche Teile der Webkonsole von Endpoint Encryption der Benutzer Zugriff hat (Power-User, Bediener oder Administrator).

Alle Benutzerkonten, die in Control Manager erstellt wurden, haben Administratorzugriff auf alle verwalteten Produkte, auf die der Benutzer Zugriff hat. Daraus ergibt sich ein Problem, wenn ein Administrator den Benutzerzugriff auf dem Endpoint Encryption System auf "Power User" reduzieren will, während der Zugriff auf Control Manager zugelassen wird.

MCP-Rückmeldung

Um den Status der verwalteten Produkte zu überwachen, fragen MCP Agents den Control Manager auf Grundlage eines Zeitplans ab. Dadurch kann der Status des

verwalteten Produkts angezeigt und überprüft werden, ob Befehle von Control Manager an das verwaltete Produkt vorliegen. Die Webkonsole von Control Manager zeigt dann den Produktstatus an. Dies bedeutet, dass der Status des verwalteten Produkts nicht in Echtzeit dargestellt wird. Control Manager überprüft sequenziell im Hintergrund den Status eines jeden verwalteten Produkts. Control Manager ändert den Status der verwalteten Produkte in Offline, wenn das verwaltete Produkt sich innerhalb eines festgelegten Zeitraums nicht zurückmeldet.

Control Manager kann den Status der verwalteten Produkte nicht nur durch aktive Rückmeldungen feststellen. Auch die folgenden Funktionen liefern Control Manager Informationen über den Status des verwalteten Produkts:

- Control Manager erhält Protokolle vom verwalteten Produkt. Wenn Control Manager erfolgreich ein Protokoll vom verwalteten Produkt empfängt, wird davon ausgegangen, dass das verwaltete Produkt ordnungsgemäß funktioniert.
- Im Zwei-Wege-Kommunikationsmodus versendet Control Manager aktiv eine Benachrichtigung an das verwaltete Produkt, damit dieses den anstehenden Befehl abruft. Wenn der Server erfolgreich eine Verbindung zum verwalteten Produkt herstellt, ist auch dies ein Anzeichen dafür, dass das Produkt ordnungsgemäß funktioniert, und dieses Ereignis zählt als Rückmeldung.
- Im Ein-Wege-Kommunikationsmodus sendet der MCP Agent periodisch Abfragebefehle an Control Manager. Dieses Verhalten entspricht einer Rückmeldung und wird von Control Manager als solche behandelt.

Die MCP-Rückmeldungen können in verschiedener Weise erfolgen:

- **UDP**: Die einfachste und schnellste Lösung ist eine Verbindung zwischen dem Produkt und dem Server über UDP. In NAT- oder Firewall-Umgebungen ist diese Lösung nicht möglich. Der Client, der die Anfrage überträgt, kann jedoch nicht überprüfen, ob der Server die Anfrage erhält.
- **HTTP/HTTPS**: In einer NAT- oder Firewall-Umgebung erfolgt die Rückmeldung über eine schwerfälligere HTTP-Verbindung.

Control Manager unterstützt die Übertragung von Rückmeldungen über UDP und HTTP/HTTPS. Control Manager Server stellt fest, welchen Modus das verwaltete Produkt während des Registrierungsvorgangs anwendet. Der Modus wird durch einen separaten Protokoll-Handshake zwischen beiden Parteien festgelegt.

Neben der Rückmeldung des Produktstatus können zusätzliche Daten an Control Manager gesendet werden. Diese Daten enthalten üblicherweise Informationen über die Aktivität des verwalteten Produkts, die auf der Konsole angezeigt werden.

Die Zeitplanleiste verwenden

Mit Hilfe der Zeitplanleiste im Fenster **Agent Communication Schedule** können Sie Communicator-Zeitpläne anzeigen und bearbeiten. Die Leiste hat 24 Positionen, von denen jede eine Stunde des Tages darstellt.

Die Felder mit den Uhrsymbolen zeigen den Arbeitsstatus bzw. die Stunden an, an dem bzw. zu denen der Agent/Communicator Informationen an den Control Manager Server senden soll. Weiße Positionen zeigen die Ruhezeit an. Definieren Sie Arbeits- oder Ruhezeiten durch die Auswahl bestimmter Positionen.

Sie können höchstens drei aufeinander folgende inaktive Zeiträume angeben. Die Schedule Bar im Beispiel unten zeigt nur zwei inaktive Zeiträume:

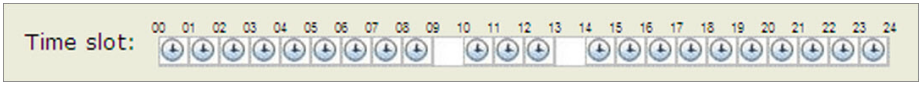


ABBILDUNG A-1. Zeitplanleiste

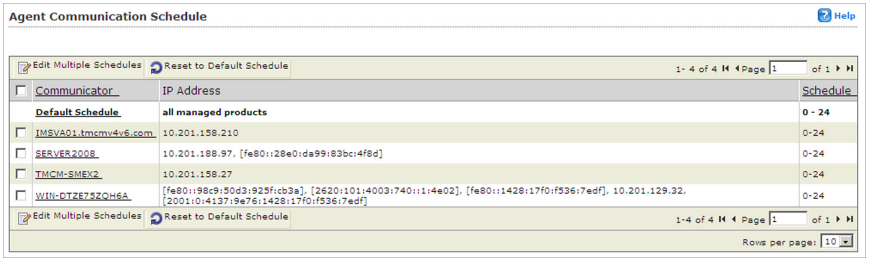
Die in der Leiste angegebenen aktiven Zeiträume sind 0:00 bis 7:00, 8:00 bis 16:00 und von 18:00 bis 24:00.

Einen Zeitplan für die Kommunikation mit Agents für ein verwaltetes Produkt festlegen

Prozedur

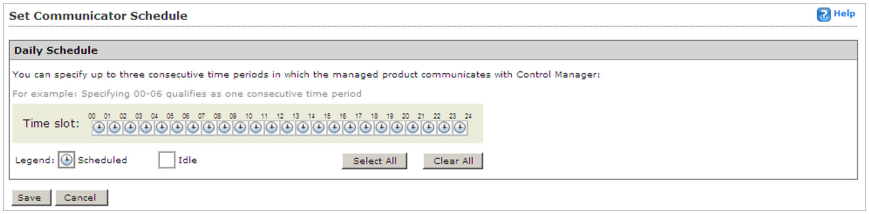
1. Öffnen Sie die Control Manager Konsole.
2. Navigieren Sie zu **Administration** > **Settings** > **Agent Communication Schedule**.

   Das Fenster **Agent Communication Schedule** wird angezeigt.



3. Wählen Sie den Zeitplan für das verwaltete Produkt, der geändert werden soll.

   Das Fenster **Set Communicator Schedule** wird angezeigt.


Set Communicator Schedule
Help
Daily Schedule
You can specify up to three consecutive time periods in which the managed product communicates with Control Manager:
For example: Specifying 00-06 qualifies as one consecutive time period
Time slot:
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Legend: Scheduled
Idle
Select All
Clear All
Save
Cancel

4. Definieren Sie den Zeitplan. Geben Sie eine neue Uhrzeit an, oder verwenden Sie die Standardeinstellung:

   - Zum Angeben einer neuen Einstellung ändern Sie die entsprechenden Zeitpositionen in der Zeitplanleiste, und klicken Sie anschließend auf **Save**
   - Wenn Sie die Standardeinstellung verwenden möchten, kehren Sie zum Fenster **Agent Communication Schedule** zurück. Wählen Sie den Zeitplan, der angewendet werden soll, und klicken Sie auf **Reset to Default Schedule**

Die richtige Einstellung für Rückmeldungen ermitteln

Bei der Einstellung der Rückmeldungen ist zu berücksichtigen, dass einerseits die neuesten Statusinformationen des verwalteten Produkts angezeigt, andererseits aber auch die Systemressourcen effizient gehandhabt werden müssen. Die Standardeinstellung bringt in den meisten Fällen zufriedenstellende Ergebnisse, Sie sollten jedoch die folgenden Punkte berücksichtigen, wenn Sie die Einstellung für die Rückmeldung anpassen:

TABELLE A-4. Empfehlungen für Rückmeldungen

ZEITINTERVALL FÜR RÜCKMELDUNGEN	EMPFEHLUNG
Lange Intervalle zwischen Rückmeldungen (mehr als 60 Minuten)	Je länger das Intervall zwischen den Rückmeldungen ist, desto größer ist die Anzahl der Ereignisse, die eintreten können, bevor Control Manager den Communicator-Status auf der Web-Konsole anzeigt. Wird z. B. ein Verbindungsproblem mit einem Communicator zwischen zwei Rückmeldungen gelöst, so kann eine Kommunikation mit einem Communicator stattfinden, selbst wenn der Status als (inaktiv) oder (unnormal) angezeigt wird.
Kurze Intervalle zwischen Rückmeldungen (weniger als 60 Minuten)	Bei kurzen Intervallen zwischen den Rückmeldungen ergibt sich auf dem Control Manger Server ein aktuelleres Bild Ihres Netzwerkstatus. Diese Option erfordert allerdings eine hohe Bandbreite.

Rückmeldung von Agent Communicator konfigurieren

Im Fenster **Communication Time-out** definieren Sie die Frequenz und die maximalen Verzögerungszeiten (in Minuten) für den Control Manager Server und die Agent-Kommunikation.

Hinweis

Die Einstellung für die Rückmeldung von Agent/Communicator gilt nur für Communicators für verwaltete Produkte, die direkt vom Control Manager Server gesteuert werden. Untergeordnete Agents/Communicators für Control Manager Server verwenden vordefinierte Werte:

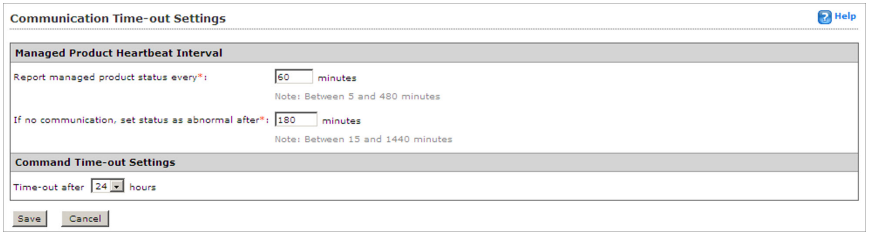
Frequency: 3 Minuten

Maximum delay: 5 Minuten

Prozedur

1. Öffnen Sie die Control Manager Konsole.
2. Navigieren Sie zu **Administration** > **Settings** > **Communication Time-out Settings**.

   Das Fenster **Communication Time-out** wird angezeigt.



3. Im Arbeitsbereich können Sie entweder die Standardwerte belassen oder neue Einstellungen für Folgendes festlegen:

   - **Report managed product status every**: Definiert, wie oft das verwaltete Produkt auf Meldungen vom Control Manager Server reagiert. Gültige Werte liegen zwischen 5 und 480 Minuten
   - **If no communication, set status as abnormal after**: Gibt an, wie lange Control Manager auf eine Antwort vom verwalteten Produkt wartet, bevor der Status der Webkonsole auf (inaktiv) geändert wird. Gültige Werte liegen zwischen 15 und 1440 Minuten.

   Hinweis

   Der Wert für **If no communication, set status as abnormal after** muss wenigstens dreimal so hoch sein wie der Wert für **Report managed product status every**.

4. Klicken Sie auf **Save**.

Grundlegendes zum Produktverzeichnis

Bei einem verwalteten Produkt handelt es sich um eine Repräsentation eines Antivirus-, Content-Sicherheit- oder Web-Schutz-Produkts im Produktverzeichnis. Verwaltete Produkte werden als Symbole (Beispiel: ( ) oder ( )) auf der Webkonsole von Control Manager, Abschnitt Produktverzeichnis, angezeigt. Diese Symbole stellen die Produkte von Trend Micro zu Antivirus, Content-Sicherheit und Schutz vor Internet-Bedrohungen dar. Control Manager unterstützt dynamische Symbole, die sich je nach Status des verwalteten Produkts ändern. Weitere Informationen zu den Symbolen und den damit in Zusammenhang stehenden Statuszuständen des verwalteten Produkts finden Sie in der Dokumentation zum betreffenden verwalteten Produkt.

Sie können verwaltete Produkte entweder individuell oder indirekt mit Hilfe von Gruppen über das Produktverzeichnis verwalten. In der folgenden Tabelle werden die Menübefehle und Schaltflächen im Fenster "Produktverzeichnis" aufgeführt.

TABELLE A-5. Optionen des Produktverzeichnisses

MENÜELEMENT	BESCHREIBUNG
Erweiterte Suche	Klicken Sie auf diesen Menübefehl, um die Suchkriterien für eine Suche nach einem oder mehreren verwalteten Produkten anzugeben.
Konfigurieren	Bewegen Sie nach der Auswahl eines verwalteten Produkts/Verzeichnisses den Mauszeiger über diesen Menübefehl, und wählen Sie eine Aufgabe aus, um sich bei einer Web-basierte Konsole mit SSO anzumelden oder ein verwaltetes Produkt zu konfigurieren.

MENÜELEMENT	BESCHREIBUNG
Aufgaben	Bewegen Sie nach der Auswahl eines verwalteten Produkts/Verzeichnisses den Mauszeiger über diesen Menübefehl, und wählen Sie eine Aufgabe aus, um eine bestimmte Funktion (wie z. B. die Verteilung der neuesten Komponenten) auf einem bestimmten verwalteten Produkt oder einem untergeordneten Server bzw. einer Gruppe von verwalteten Produkten oder untergeordneten Server auszuführen. Sie können eine Aufgabe aus einem Verzeichnis heraus initiieren. Daraufhin sendet Control Manager Anforderungen an alle verwalteten Produkte, die zu diesem Verzeichnis gehören.
Verzeichnisverwaltung	Klicken Sie auf diese Schaltfläche, um das Fenster **Directory Management** zu öffnen. In diesem Fenster können Sie Elemente/ Verzeichnisse verschieben (indem Sie sie ziehen und ablegen) oder neue Verzeichnisse erstellen.
Schaltflächen	
Suchen	Klicken Sie auf diese Schaltfläche, nachdem Sie den Namen eines verwalteten Produkts eingegeben haben, um nach dem angegebenen verwalteten Produkt zu suchen.
Status	Klicken Sie auf diese Schaltfläche, nachdem Sie ein verwaltetes Produkt/ Verzeichnis ausgewählt haben, um Statuszusammenfassungen über das bzw. die verwalteten Produkte im Verzeichnis abzurufen.

MENÜELEMENT	BESCHREIBUNG
Ordner	Klicken Sie auf diese Schaltfläche, nachdem Sie ein Verzeichnis ausgewählt haben, um Statuszusammenfassungen über das bzw. die verwalteten Produkte und die Endpunkte der verwalteten Produkte im Verzeichnis abzurufen.

Hinweis

Sie können verwalteten Produkten, die zu untergeordneten Control Manager Servern gehören, keine Aufgaben vom übergeordneten Control Manager Server zuweisen.

Empfehlungen zur Struktur des Produktverzeichnisses

Bei der Planung der Struktur des Produktverzeichnisses für verwaltete Produkte und untergeordnete Server empfiehlt Trend Micro Folgendes:

TABELLE A-6. Überlegungen zur Gruppierung von verwalteten Produkte oder untergeordneten Servern

STRUKTUR	BESCHREIBUNG
Netzwerk- und Sicherheitsrichtlinien des Unternehmens	Wenn für das Unternehmensnetzwerk unterschiedliche Zugriffs- und Freigaberechte gelten, sollten Sie die verwalteten Produkte und untergeordneten Server entsprechend den Netzwerk- und Sicherheitsrichtlinien des Unternehmens gruppieren.
Organisation und Funktion	Sie können verwaltete Produkte und untergeordnete Server entsprechend den organisatorischen und funktionalen Abteilungen gruppieren. Sie können z. B. zwei Control Manager Server einsetzen, um die Gruppen Produktion und Tests zu verwalten.

STRUKTUR	BESCHREIBUNG
Geografische Lage	Sie können die geografische Lage als Kriterium für die Gruppierung verwenden, wenn der Standort der verwalteten Produkte und untergeordneten Server sich auf die Kommunikation zwischen dem Control Manager Server und seinen verwalteten Produkten oder untergeordneten Server auswirkt.
Verwaltungszuständigkeit	Sie können verwaltete Produkte und untergeordnete Server entsprechend dem System- oder Sicherheitspersonal gruppieren, dem sie zugeordnet sind. Dies ermöglicht die Konfiguration von Gruppen.

Das Produktverzeichnis stellt eine benutzerdefinierte Gruppierung der verwalteten Produkte bereit, durch die Sie in die Lage versetzt werden, die folgenden Funktionen bei der Administrierung von verwalteten Produkten auszuführen:

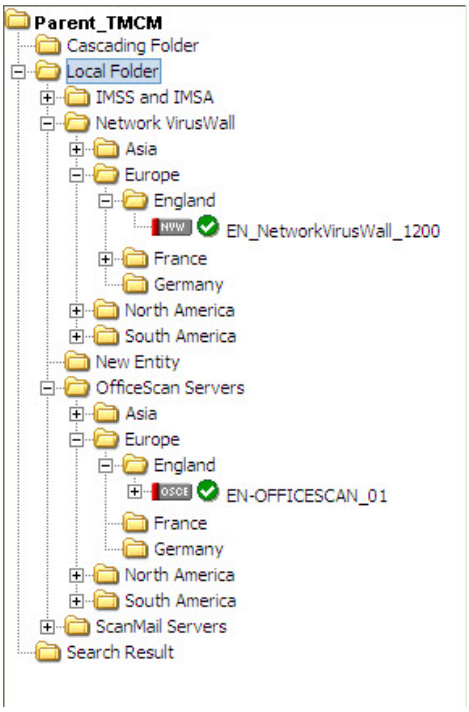
- Verwaltete Produkte konfigurieren
- Produkte anweisen, die Funktion "Jetzt durchsuchen" auszuführen (wenn dieser Befehl unterstützt wird)
- Produktinformationen sowie Details zur Betriebsumgebung anzuzeigen (Beispiel: Produktversion, Pattern-Datei und Scan-Engine-Versionen, Betriebssysteminformationen usw.)
- Protokolle auf Produktebene anzuzeigen
- Viren-Pattern, Scan Engines, Anti-Spam-Regeln und Programmaktualisierungen zu verteilen

Gehen Sie bei der Planung dieser Struktur sorgsam um, denn die Struktur wirkt sich auch auf Folgendes aus:

TABELLE A-7. Überlegungen zur Struktur

ÜBERLEGUNG	WIRKUNG
Benutzerzugriff	Bei der Erstellung von Benutzerkonten fordert der Control Manager zur Eingabe des Produktverzeichnis-Segments auf, auf das der Benutzer Zugriff hat. Mit einer Zugriffsberechtigung auf das Stammsegment erhalten Sie zum Beispiel Zugriff auf das gesamte Verzeichnis. Durch die Gewährung von Zugriff auf ein bestimmtes verwaltetes Produkt erhalten Sie nur Zugriff auf dieses Produkt.
Installation und Verteilung planen	Control Manager verteilt aktualisierte Komponenten (Beispiel: Viren-Pattern-Dateien, Scan Engines, Anti-Spam-Regeln, Programmaktualisierungen) auf Grundlage des Verteilungsplans an die Produkte. Laut diesen Plänen werden die Komponenten an Produktverzeichnisordner und nicht an individuelle Produkte verteilt. Ein gut strukturiertes Verzeichnis erleichtert daher die Festlegung der Empfänger.
Verteilung von Präventionsrichtlinien (OPP) und Damage Cleanup Templates (DCT)	Die OPP- und DCT-Verteilung erfordert Verteilungspläne zur effizienten Verteilung der Präventionsrichtlinie und der Säuberungsaufgaben.

Ein Beispiel für ein Produktverzeichnis sehen Sie weiter unten:



Verwaltete Produkte identifizieren das registrierte Antiviren- und Content-Security-Produkt und stellen außerdem den Verbindungsstatus bereit.

Hinweis

Unabhängig vom Agent-Typ werden neu registrierte verwaltete Produkte im Ordner "Neues Element" angezeigt.

TABELLE A-8. Symbole für verwaltete Produkte

SYMBOL	BESCHREIBUNG
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	ServerProtect Information Server
	ServerProtect Domain
NT	ServerProtect for Windows (normaler Server)

SYMBOL	BESCHREIBUNG
	ServerProtect for NetWare (normaler Server)
	InterScan Messaging Security Suite
	InterScan Web Security Suite
	InterScan VirusWall für Windows
	InterScan VirusWall für UNIX
	ScanMail for Microsoft Exchange
	ScanMail für Lotus Notes
	Network VirusWall
	NetScreen Global PRO Firewall
	Symbol für den Verbindungsstatus verwalteter Produkte

Ordnen Sie das Produktverzeichnis mit Hilfe des Directory Managers. Verwenden Sie beschreibende Ordnernamen, um Ihre verwalteten Produkte nach der Art ihres Schutzes und dem Netzwerk-Administrationsmodell von Control Manager zu gruppieren.

Auf das Produktverzeichnis zugreifen

Beim Control Manager Server registrierte verwaltete Produkte werden über das Produktverzeichnis verwaltet.

Hinweis

Die Anzeige und der Zugriff auf Ordner im Produktverzeichnis hängt vom Kontotyp und den Zugriffsrechten des Benutzerkontos ab.

Prozedur

- Klicken Sie im Hauptmenü auf **Products**.

Das Fenster **Product Directory** wird angezeigt.

Komponenten mit dem Produktverzeichnis manuell verteilen

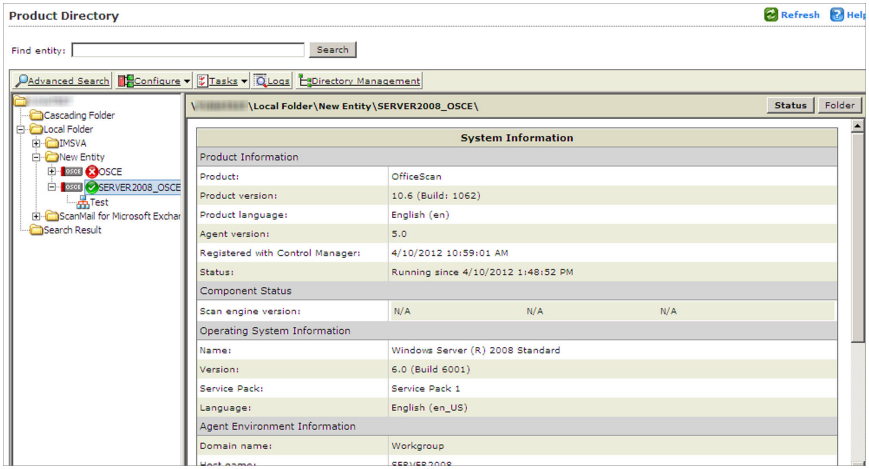
Über manuelle Verteilungen können Sie Viren-Pattern, Spam-Regeln und Scan Engines der verwalteten Produkte bei Bedarf aktualisieren. Setzen Sie diese Methode ein, um Komponenten während eines Virenausbruchs zu aktualisieren.

Laden Sie die neuen Komponenten herunter, bevor Sie Aktualisierungen auf ein bestimmtes verwaltetes Produkt oder Gruppen von verwalteten Produkten verteilen.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.



2. Wählen Sie ein verwaltetes Produkt oder ein Verzeichnis aus dem Produktverzeichnis.

   Das verwaltete Produkt oder Verzeichnis wird hervorgehoben.

3. Bewegen Sie den Mauszeiger über **Tasks** im Menü "Produktverzeichnis".
4. Wählen Sie aus dem Dropdown-Menü **Deploy <component>**.
5. Klicken Sie auf **Deploy Now**, um die manuelle Verteilung neuer Komponenten zu starten.
6. Überwachen Sie den Fortschritt über das Fenster **Command Tracking**.
7. Klicken Sie im Fenster **Command Tracking** auf den Link "Befehlsdetails", um Details für die Aufgabe "Sofort verteilen" anzuzeigen.

Statuszusammenfassungen für verwaltete Produkte anzeigen

Im Fenster "Produktstatus" werden Zusammenfassungen zu Antivirus, Content-Sicherheit und Web Security für alle verwalteten Produkte angezeigt, die sich in der Struktur des Produktverzeichnisses befinden.

Es gibt zwei Methoden, um die Statuszusammenfassung der verwalteten Produkte anzuzeigen:

- Über das Dashboard mit dem Widget "Ergebnisse der Bedrohungserkennung" (das sich auf der Registerkarte "Zusammenfassung" befindet)
- Über das Produktverzeichnis

Über das Dashboard zugreifen

Prozedur

- Beim Öffnen der Webkonsole von Control Manager wird auf dem Dashboard die Registerkarte **Summary** mit einer Zusammenfassung des gesamten Control Manager Netzwerks angezeigt. Diese Zusammenfassung ist identisch mit der Anzeige auf der Registerkarte Produktstatus im Stammordner des Produktverzeichnisses.

Über das Produktverzeichnis zugreifen

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie aus der Struktur des Produktverzeichnisses den gewünschten Ordner oder das gewünschte verwaltete Produkt aus.

   - Beim Klicken auf ein verwaltetes Produkt wird auf der Registerkarte "Produktstatus" eine Zusammenfassung des verwalteten Produkts angezeigt.
   - Wenn Sie auf den Stammordner, den Ordner "Neues Element" oder einen anderen benutzerdefinierten Ordner klicken, werden auf der Registerkarte "Produktstatus" die Zusammenfassungen zu Antivirus, Content-Sicherheit und Web Security angezeigt.

   Hinweis

   Standardmäßig werden im Status Summary die Informationenen einer Woche bis zum Tag Ihrer Abfrage angezeigt. Sie können die Einstellungen **Today**, **Last Week**, **Last Two Weeks** oder **Last Month** unter "Zusammenfassung für Liste anzeigen" ändern.

Verwaltete Produkte konfigurieren

Abhängig von der Produkt- und Agent-Version können Sie das verwaltete Produkt von der Webkonsole des verwalteten Produkts oder über eine von Control Manager generierte Konsole konfigurieren.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie das gewünschte verwaltete Produkt aus dem Produktverzeichnis aus.

Der Produktstatus wird im rechten Fensterbereich angezeigt.

3. Bewegen Sie den Mauszeiger über **Configure** im Menü "Produktverzeichnis".
4. Wählen Sie eine der folgenden Optionen:

   - **Configuration Replication**: Das Fenster **Configuration Settings** wird angezeigt.

     a. Wählen Sie den Ordner, in den die Einstellungen des verwalteten Produkts aus dem Produktverzeichnis repliziert werden sollen.

     b. Klicken Sie auf **Replicate**.

     Die Einstellungen des ausgewählten verwalteten Produkts werden auf den verwalteten Zielprodukten repliziert.

   - **<Managed Product Name> Single Sign On**: Die Webkonsole des verwalteten Produkts oder die von Control Manager generierte Konsole wird angezeigt.

     a. Sie können das verwaltete Produkt über die Webkonsole konfigurieren.

Hinweis

Weitere Informationen zur Konfiguration von verwalteten Produkten finden Sie in der Dokumentation des verwalteten Produkts.

Aufgaben für verwaltete Produkte

Mit dem Menübefehl "Aufgaben" rufen Sie die verfügbaren Aktionen für ein bestimmtes verwaltetes Produkt auf. Abhängig vom verwalteten Produkt sind alle oder einige der folgenden Aufgaben verfügbar:

- Engines verteilen und installieren
- Pattern-Dateien/Cleanup-Templates verteilen und installieren
- Programmdateien verteilen und installieren
- Echtzeitsuche aktivieren oder deaktivieren

- Jetzt suchen starten

Sie können die letzten Spam-Regeln, Pattern oder Scan Engines an verwaltete Produkte mit veralteten Komponenten verteilen. Dazu müssen auf dem Control Manager Server die aktuellen, auf dem Trend Micro ActiveUpdate Server verfügbaren Komponenten vorliegen. Stellen Sie dies über einen manuellen Download sicher.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie das verwaltete Produkt oder Verzeichnis, um eine Aufgabe zu erteilen.

3. Bewegen Sie den Mauszeiger über **Tasks**.

4. Klicken Sie auf eine Aufgabe aus der Liste. Überwachen Sie den Fortschritt über das Command Tracking. Klicken Sie im angezeigten Fenster auf den Link **Command Details**, um weitere Einzelheiten zum Befehl anzuzeigen.

Protokolle für verwaltete Produkte abfragen und anzeigen

Über die Registerkarte "Protokolle" können Sie die Protokolle für eine Gruppe oder ein bestimmtes verwaltetes Produkt abfragen und anzeigen.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

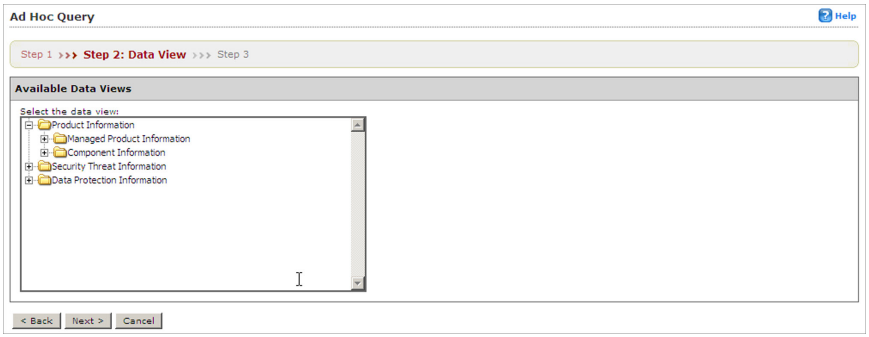
   Das Fenster **Product Directory** wird angezeigt.

2. Wählen Sie das gewünschte verwaltete Produkt oder einen Ordner aus dem Produktverzeichnis.

3. Bewegen Sie den Mauszeiger über **Logs** im Menü "Produktverzeichnis".

4. Klicken Sie im Dropdown-Menü auf **Logs**.

   Das Fenster **Ad Hoc Query > Step 2: Select Data View** wird angezeigt.

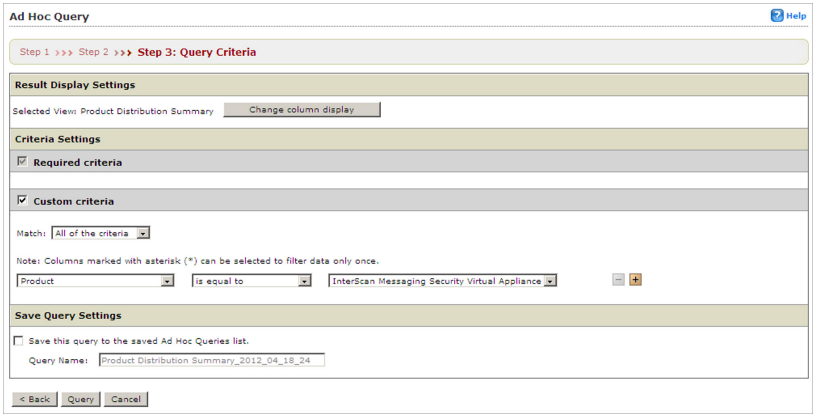


5. Geben Sie die Datenansicht für das Protokoll an:

   a. Wählen Sie die abzufragenden Daten aus dem Bereich "Verfügbare Datenansichten".

   b. Klicken Sie auf **Next**.

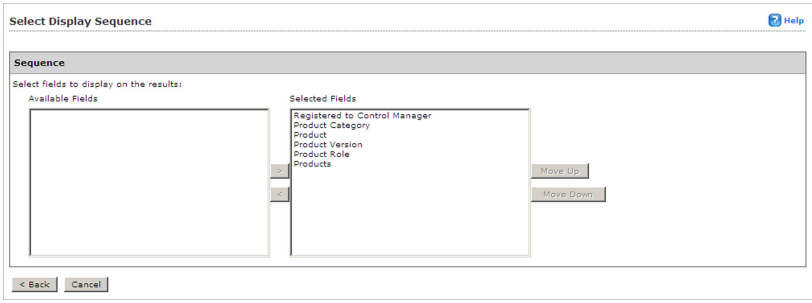
      Das Fenster **Ad Hoc Query > Step 3: Query Criteria** wird angezeigt.


Ad Hoc Query
Help
Step 1 ››› Step 2 ››› Step 3: Query Criteria
Result Display Settings
Selected View: Product Distribution Summary
Change column display
Criteria Settings
Required criteria
Custom criteria
Match: All of the criteria
Note: Columns marked with asterisk (*) can be selected to filter data only once.
Product
is equal to
InterScan Messaging Security Virtual Appliance
Save Query Settings
Save this query to the saved Ad Hoc Queries list.
Query Name: Product Distribution Summary_2012_04_18_24
< Back
Query
Cancel

6. Geben Sie die Daten und die Reihenfolge an, in der sie im Protokoll angezeigt werden sollen. Elemente, die oben in der Liste "Ausgewählte Felder" angezeigt werden, werden in der Tabelle in der äußerst linken Spalte angezeigt. Wenn Sie ein Feld aus der Liste "Ausgewählte Felder" entfernen, wird auch die entsprechende Spalte aus der von der Ad-hoc-Abfrage zurückgegebenen Tabelle entfernt.

a. Klicken Sie auf **Change column display**.

Das Fenster **Select Display Sequence** wird angezeigt.



b. Wählen Sie eine Abfragespalte aus der Liste "Verfügbare Felder". Sie können mehrere Elemente durch Drücken der **Shift**- oder **Ctrl**-Taste auswählen.

c. Klicken Sie auf **>**, um Elemente der Liste "Ausgewählte Felder" hinzuzufügen.

d. Legen Sie die Reihenfolge fest, in der Daten angezeigt werden sollen, indem Sie das betreffende Element auswählen und auf **Move up** oder **Move down** klicken.

e. Klicken Sie auf **Back**, wenn die Reihenfolge Ihren Anforderungen entspricht.

7. Geben Sie die Filterkriterien für die Daten an:

Hinweis

Wenn Sie eine Abfrage für zusammenfassende Daten definieren, müssen Sie die Elemente unter "Erforderliche Kriterien" angeben.

- Erforderliche Kriterien:
  - Geben Sie eine Uhrzeit für die Zusammenfassung der Daten an oder legen Sie fest, ob COOKIES in Ihren Berichten erscheinen sollen.
- Benutzerdefinierte Kriterien:
  a. Geben Sie die Regeln für die Filterkriterien für die Datenkategorien an:

- **All of the criteria**: Diese Auswahl dient als logische UND-Funktion. Die im Bericht angezeigten Daten müssen alle Filterkriterien erfüllen.
- **Any of the criteria**: Diese Auswahl dient als logische ODER-Funktion. Die im Bericht angezeigten Daten müssen beliebige Filterkriterien erfüllen.

b. Geben Sie die Filterkriterien für die Daten an. Control Manager unterstützt die Angabe von bis zu 20 Kriterien für die Filterung von Daten.

Tipp

Wenn Sie keine Filterkriterien angeben, gibt die Ad-hoc-Abfrage alle Ergebnisse für die entsprechenden Spalten zurück. Trend Micro empfiehlt die Angabe von Filterkriterien zur Vereinfachung der Datenanalyse, nachdem die Informationen für die Abfrage zurückgegeben wurden.

8. Speichern Sie die Abfrage:

a. Klicken Sie auf **Save this query to the saved Ad Hoc Queries list**.

b. Geben Sie den Namen für die gespeicherte Abfrage in das Feld **Query Name** ein.

9. Klicken Sie auf **Query**.

Das Fenster **Results** wird angezeigt.

10. Speichern Sie den Bericht als .CSV-Datei:

a. Klicken Sie auf **Export to CSV**.

b. Klicken Sie auf **Download**.

c. Geben Sie den Speicherort für die Datei an.

d. Klicken Sie auf **Save**.

11. Speichern Sie den Bericht als .XML-Datei:

a. Klicken Sie auf **Export to XML**.

b. Klicken Sie auf **Download**.

c. Geben Sie den Speicherort für die Datei an.

d. Klicken Sie auf **Save**.

Tipp

Um die Anzahl der in einem Fenster angezeigten Abfrageergebnissen zu erhöhen, wählen Sie einen anderen Wert für " Zeilen pro Seite". In einem einzelnen Fenster können 10, 15, 30 oder 50 Suchabfrageergebnisse pro Seite angezeigt werden.

12. Speichern Sie die Einstellungen für die Abfrage:

a. Klicken Sie auf **Save query settings**.

b. Geben Sie den Namen für die gespeicherte Abfrage in das Feld **Query Name** ein.

c. Klicken Sie auf **OK**.

Die gespeicherte Abfrage wird im Fenster **Saved Ad Hoc Queries** angezeigt.

Informationen zum Wiederherstellen von verwalteten Produkten, die aus dem Produktverzeichnis entfernt wurden

Die folgenden Szenarien können dazu führen, dass der Control Manager verwaltete Produkte aus dem Produktverzeichnis löscht:

- Der Control Manager Server wird neu installiert, und der Befehl **Delete existing records and create a new database** wird ausgewählt

  Bei dieser Option wird eine neue Datenbank mit dem Namen der bestehenden Datenbank erstellt.

- Die beschädigte Control Manager Datenbank wird durch eine andere Datenbank mit dem gleichen Namen ersetzt.

- Das verwaltete Produkt wird versehentlich aus der Verzeichnisverwaltung gelöscht

Auch wenn auf einem Control Manager Server keine Einträge zu verwalteten Produkten mehr angezeigt werden, "wissen" die TMI Agents auf den Produkten trotzdem, wo sie registriert sind. Der Control Manager Agent registriert sich nach acht Stunden oder beim Neustart des Dienstes automatisch erneut.

MCP Agents führen keine automatische Neuregistrierung durch. Administratoren müssen die Neuregistrierung von verwalteten Produkten mit Hilfe von MCP Agents manuell durchführen.

Verwaltete Produkte wiederherstellen, die aus dem Produktverzeichnis entfernt wurden

Prozedur

- Starten Sie den Trend Micro Control Manager Dienst auf dem Server des verwalteten Produkts neu. Weitere Informationen finden Sie unter *Control Manager Dienste anhalten und neu starten auf Seite A-33*.
- Warten Sie, bis der Agent sich erneut registriert hat: Standardmäßig überprüfen ältere Control Manager Agents ihre Verbindung zum Server alle acht Stunden. Wenn der Agent erkennt, dass sein Datensatz gelöscht wurde, registriert er sich automatisch erneut.
- Manuelle Neuregistrierung bei Control Manager: MCP Agents führen keine automatische Neuregistrierung durch und müssen manuell beim Control Manager Server erneut registriert werden.

Control Manager Dienste anhalten und neu starten

Im Fenster **Windows Services** können Sie die folgenden Control Manager Dienste neu starten:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager

Hinweis

Diese Dienste laufen unter dem Windows-Betriebssystem im Hintergrund. Es handelt sich dabei nicht um Trend Micro Dienste, die einen Aktivierungscode erfordern (Beispiel: Outbreak Prevention Services).

Prozedur

1. Klicken Sie auf **Start** > **Programs** > **Administrative Tools** > **Services**, um das Fenster **Services** zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf **<Control Manager service>**, und klicken Sie anschließend auf **Stop**.
3. Klicken Sie mit der rechten Maustaste auf **<Control Manager service>**, und klicken Sie anschließend auf **Start**.

Nach verwalteten Produkten, Ordnern im Produktverzeichnis oder Computern suchen

Mit Hilfe der Schaltfläche **Search** können Sie im Produktverzeichnis ein bestimmtes verwaltetes Produkt schnell ausfindig machen.

Nach einem Ordner oder verwalteten Produkt suchen

Prozedur

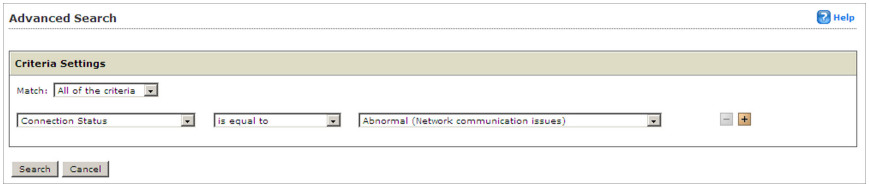
1. Öffnen Sie das Produktverzeichnis.
2. Geben Sie den Anzeigenamen des verwalteten Produkts in das Feld **Find entity** ein.
3. Klicken Sie auf **Search**.

Erweiterte Suche durchführen

Prozedur

1. Öffnen Sie das Produktverzeichnis.
2. Klicken Sie auf **Advanced Search**.

   Das Fenster **Advanced Search** wird angezeigt.



3. Geben Sie die Filterkriterien für das Produkt an. Control Manager unterstützt die Angabe von bis zu 20 Kriterien für die Durchführung von Recherchen.
4. Klicken Sie auf **Search**, um mit der Suche zu beginnen.

   Die Suchergebnisse werden im Produktverzeichnis im Ordner **Search Result** angezeigt.

Das Produktverzeichnis aktualisieren

Prozedur

- Klicken Sie in der rechten oberen Fensterecke im Fenster **Product Directory** auf das Symbol **Refresh**.

Grundlegendes zum Fenster "Verzeichnisverwaltung"

Nach der Registrierung beim Control Manager wird das verwaltete Produkt im Standardordner im Produktverzeichnis angezeigt.

Mit dem Fenster "Verzeichnisverwaltung" können Sie die Struktur des Produktverzeichnisses an Ihre Anforderungen anpassen. Sie können beispielsweise Produkte nach Speicherort oder Produkttyp (Messaging Security, Web Security, Dateispeicherschutz) gruppieren.

Im Produktverzeichnis können Sie Ordner erstellen, ändern oder löschen und verwaltete Produkte von einem Ordner in einen anderen verschieben. Allerdings können Sie den Ordner New entity weder löschen noch umbenennen.

Richten Sie die verwalteten Produkte, die jeweils zu einem Ordner gehört, sorgfältig ein. Berücksichtigen Sie bei der Planung und Implementierung der Struktur Ihrer Ordner und verwalteten Produkte die folgenden Faktoren:

- Produktverzeichnis
- Benutzerkonten
- Verteilungspläne
- Ad-hoc-Abfrage
- Control Manager Berichte

Sie können verwaltete Produkte nach geografischen, administrativen oder produktspezifischen Aspekten gruppieren. In der folgenden Tabelle finden Sie die empfohlenen Gruppierungstypen sowie deren Vor- und Nachteile in Kombination mit verschiedenen Zugriffsrechten zum Zugriff auf verwaltete Produkte oder Ordner im Verzeichnis.

TABELLE A-9. Vergleich der Produktgruppierungen

GRUPPIERUNGSTYP	VORTEILE	NACHTEILE
Geografisch oder administrativ	Klare Struktur	Keine Gruppenkonfiguration für identische Produkte
Produkttyp	Gruppenkonfiguration und Status ist verfügbar	Zugriffsrechte stimmen möglicherweise nicht überein
Kombination von beidem	Gruppenkonfiguration und Verwaltung von Zugriffsrechten	Komplexe Struktur, möglicherweise nicht leicht zu verwalten

Optionen im Fenster "Verzeichnisverwaltung" verwenden

Mit diesen Optionen können Sie verwaltete Produkte in Ihrem Control Manager Netzwerk bearbeiten und organisieren.

Das Fenster **Directory Management** enthält mehrere Optionen:

- Verzeichnisse zum Produktverzeichnis hinzufügen
- Verzeichnisse im Produktverzeichnis umbenennen
- Verwaltete Produkte oder Verzeichnisse im Produktverzeichnis verschieben
- Verwaltete Produkte oder Verzeichnisse aus dem Produktverzeichnis entfernen

Hinweis

Aktivieren Sie das Kontrollkästchen "Berechtigungen beibehalten", wenn der Ordner die Berechtigungen seiner Quelle beim Verschieben behalten soll.

Fenster "Verzeichnisverwaltung" verwenden

Prozedur

- Wählen Sie ein verwaltetes Produkt oder ein Verzeichnis, und klicken Sie auf **Rename**, um das verwaltete Produkt oder das Verzeichnis umzubenennen.
- Klicken Sie auf das **+** oder den Ordner, um die verwalteten Produkte anzuzeigen, die zu einem Ordner gehören.
- Sie können verwaltete Produkte oder Verzeichnisse durch Ziehen in das Produktverzeichnis verschieben.
- Klicken Sie auf **Add Folder** , um dem Produktverzeichnis ein Verzeichnis hinzuzufügen.

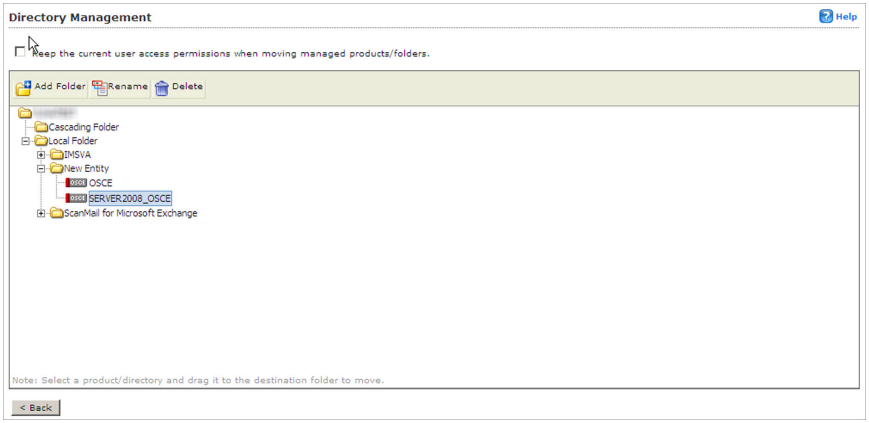
Das Fenster "Verzeichnisverwaltung" öffnen

Im Fenster **Directory Management** gruppieren Sie verwaltete Produkte.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.



2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

Ordner erstellen

Sie können die verwalteten Produkte gemäß der Netzwerkverwaltung Ihres Control Managers in verschiedene Ordner gruppieren.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie **Local Folder**.

4. Klicken Sie auf **Add Folder**.

   Das Fenster **Add Directory** wird angezeigt.

5. Geben Sie den Namen für das neue Verzeichnis in das Feld **Directory name** ein.

6. Klicken Sie auf **Save**.

Hinweis

Außer dem Ordner **New Entity** listet der Control Manager alle anderen Ordner in aufsteigender Reihenfolge auf, beginnend mit Sonderzeichen (!, #, $, %, (,), *, +, -, Komma, Punkt, +, ?, @, [,], ^, _, {, |, } und ~), Zahlen (0 bis 9) oder alphabetischen Zeichen (a/A bis z/Z).

Ordner oder verwaltete Produkte umbenennen

Sie können Verzeichnisse und verwaltete Produkte im Fenster **Directory Management** umbenennen.

Hinweis

Bei der Umbenennung eines verwalteten Produkts wird nur der in der Control Manager Datenbank gespeicherte Name geändert; die Umbenennung wirkt sich nicht auf das verwaltete Produkt aus.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie das verwaltete Produkt oder Verzeichnis, das umbenannt werden soll.

4. Klicken Sie auf **Rename**.

   Das Fenster **Rename Directory** wird angezeigt.

5. Geben Sie den Namen für das verwaltete Produkt bzw. Verzeichnis in das Feld **Directory name** ein.

6. Klicken Sie auf **Save**.

7. Klicken Sie auf **OK**.

   Das verwaltete Produkt bzw. Verzeichnis wird unter dem neuen Namen im Produktverzeichnis angezeigt.

Ordner oder verwaltete Produkte verschieben

Achten Sie beim Verschieben von Ordnern besonders auf das Kontrollkästchen **Keep the current user access permissions when moving managed products/folders**. Wenn Sie dieses Kontrollkästchen aktivieren und ein verwaltetes Produkt oder einen Ordner verschieben, behält das verwaltete Produkt oder der Ordner die Berechtigungen des Quellenordners bei. Wenn Sie das Kontrollkästchen deaktivieren und anschließend ein verwaltetes Produkt oder einen Ordner verschieben, übernimmt das verwaltete Produkt oder der Ordner die Zugriffsberechtigungen vom neuen übergeordneten Ordner.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie im Arbeitsbereich den zu verschiebenden Ordner oder das zu verschiebende verwaltete Produkt.

4. Ziehen Sie den Ordner oder das verwaltete Produkt auf den neuen Zielspeicherort.

5. Klicken Sie auf **Save**.

Benutzerdefinierte Ordner löschen

Seien Sie vorsichtig beim Löschen benutzerdefinierter Ordner im Fenster **Directory Management**. Sie könnten versehentlich ein verwaltetes Produkt löschen und damit seine Registrierung beim Control Manager Server rückgängig machen.

Hinweis

Der Ordner **New Entity** kann nicht gelöscht werden.

Prozedur

1. Klicken Sie im Hauptmenü auf **Products**.

   Das Fenster **Product Directory** wird angezeigt.

2. Klicken Sie im Menü "Produktverzeichnis" auf **Directory Management**.

   Das Fenster **Directory Management** wird angezeigt.

3. Wählen Sie das verwaltete Produkt oder Verzeichnis, das gelöscht werden soll.

4. Klicken Sie auf **Delete**.

   Ein Bestätigungsdialogfeld wird angezeigt.

5. Klicken Sie auf **OK**.

6. Klicken Sie auf **Save**.

Neue Komponenten herunterladen und verteilen

Trend Micro empfiehlt die Aktualisierung der Komponenten für Virenschutz und Content-Sicherheit, um vor Gefahren durch aktuelle Viren- und Malware-Bedrohungen geschützt zu sein.

Standardmäßig aktiviert Control Manager nur das Herunterladen von Komponenten, die zu verwalteten Produkten gehören, die im Control Manager Server registriert sind.

Control Manager aktiviert das Herunterladen von Viren-Pattern-Dateien, selbst wenn keine verwalteten Produkte im Control Manager Server registriert sind.

Die folgenden Komponenten sind zu aktualisieren (aufgeführt entsprechend der Häufigkeit der empfohlenen Aktualisierung).

TABELLE A-10. Verfügbare Komponenten

KOMPONENTE	BESCHREIBUNG
Pattern-Dateien/Cleanup-Templates	Pattern-Dateien/Cleanup-Templates enthalten Hunderte von Malware-Signaturen (Beispiel: Viren oder Trojaner) und bestimmen die Fähigkeit des verwalteten Produkts, bösartige Dateiinfektionen zu erkennen und zu säubern
Anti-Spam-Regeln	Bei den Anti-Spam-Regeln handelt es sich um Dateien, die von Trend Micro bereitgestellt werden, und die für die Anti-Spam- und Content-Filterung verwendet werden.
Engines	Engines beziehen sich auf die Scan Engines für Viren/Malware, die Damage Cleanup Engine, die VirusWall Engines, die Spyware/Grayware Engine usw. Diese Komponenten führen die eigentlichen Funktionen zum Suchen und Säubern aus.

KOMPONENTE	BESCHREIBUNG
OfficeScan Plug-in-Programme	OfficeScan Plug-in-Programme (Beispiel: Trend Micro Security for Mac). **Hinweis** Auf der OfficeScan Webkonsole werden alle verfügbaren Plug-in-Programme angezeigt. Sie können angeben, welche der Plug-in-Programme von Control Manager heruntergeladen werden. Möglicherweise wurde jedoch das betreffende Plug-in-Programm nicht von Control Manager heruntergeladen. Das bedeutet, OfficeScan kann das angegebene Plug-in-Programm nicht von Control Manager herunterladen. Überprüfen Sie vor der Angabe eines Plug-in-Programms zum Download vom Control Manager nach OfficeScan, ob Control Manager das Plug-in-Programm bereits heruntergeladen hat.
Produktprogramme und Widget-Pool	Produktspezifische Komponenten (Beispiel: Service-Pack-Veröffentlichungen) und der Control Manager Widget-Pool

Hinweis

Nur registrierte Benutzer haben ein Anrecht auf Komponenten-Updates.

Um den Netzwerkverkehr von Control Manager zu minimieren, deaktivieren Sie das Herunterladen von Komponenten, für die es kein entsprechendes verwaltetes Produkt gibt.

Das Fenster **Component List** enthält eine vollständige Liste aller Komponenten, die Control Manager für verwaltete Produkte verfügbar hat. In der Liste werden ferner Komponenten mit verwalteten Produkten abgestimmt, die die entsprechende

Komponente verwenden. Klicken Sie auf **Updates** > **Component List**, um das Fenster **Component List** zu öffnen.

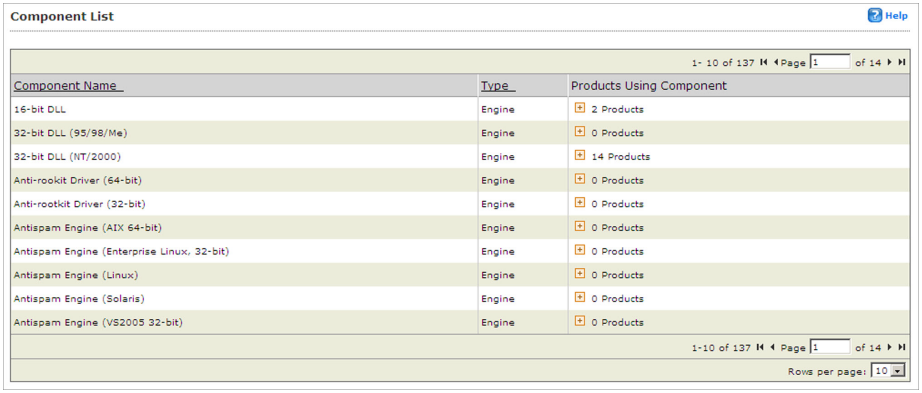


ABBILDUNG A-2. Das Fenster "Komponentenliste"

Auf dem Control Manager Server wird nur die letzte Version der Komponente gespeichert. Informationen zum Versionsverlauf einer Komponente finden Sie unter `Stamm>:\Program Files\Trend Micro\Control Manager\AU_log \TmuDump.txt`. `TmuDump.txt` wird generiert, wenn ActiveUpdate-Debugging aktiviert ist.

Tipp

Um den Netzwerkverkehr von Control Manager zu minimieren, deaktivieren Sie das Herunterladen von Komponenten, für die es kein entsprechendes verwaltetes Produkt oder keinen entsprechenden Dienst gibt. Wenn Sie zu einem späteren Zeitpunkt verwaltete Produkte registrieren oder Dienste aktivieren, vergessen Sie nicht, das manuelle oder zeitgesteuerte Herunterladen der entsprechenden Komponenten zu konfigurieren.

Komponenten manuell herunterladen

Laden Sie Komponenten-Updates manuell herunter, wenn Sie den Control Manager zum ersten Mal installieren, wenn Ihr Netzwerk angegriffen wird oder wenn Sie neue Komponenten vor der Verteilung in Ihrem Netzwerk testen möchten.

Trend Micro empfiehlt die folgende Methode zum Konfigurieren von manuellen Downloads. Der manuelle Komponenten-Download erfordert mehrere Schritte:

Tipp

Überspringen Sie Schritt 1 und 2, wenn Sie Ihren Verteilungsplan und Ihre Proxy-Einstellungen bereits konfiguriert haben.

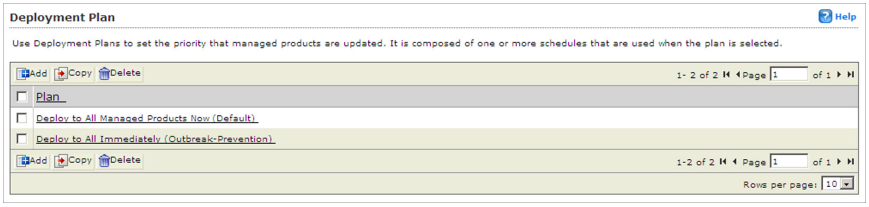
- Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.
- Schritt 2: Konfigurieren Sie Ihre Proxy-Einstellungen, wenn Sie einen Proxy-Server verwenden.
- Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.
- Schritt 4: Konfigurieren Sie die Download-Einstellungen.
- Schritt 5: Konfigurieren Sie die Einstellungen für die automatische Verteilung.
- Schritt 6: Schließen Sie den manuellen Download ab.

Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.

Prozedur

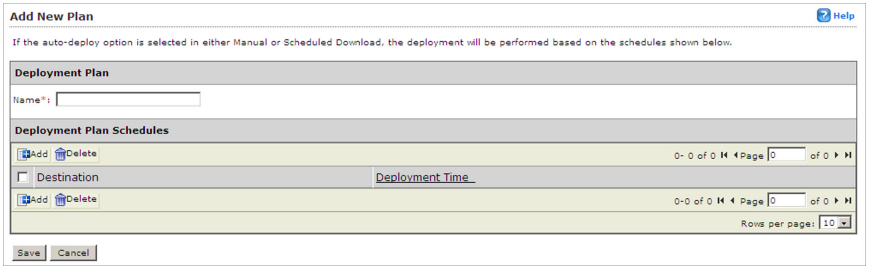
1. Navigieren Sie zu **Updates** > **Deployment Plan**.

   Das Fenster **Deployment Plan** wird angezeigt.


Deployment Plan
Help
Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.
Add
Copy
Delete
1- 2 of 2
Page 1 of 1
Plan
Deploy to All Managed Products Now (Default)
Deploy to All Immediately (Outbreak-Prevention)
Add
Copy
Delete
1-2 of 2
Page 1 of 1
Rows per page: 10

2. Klicken Sie auf **Add**.

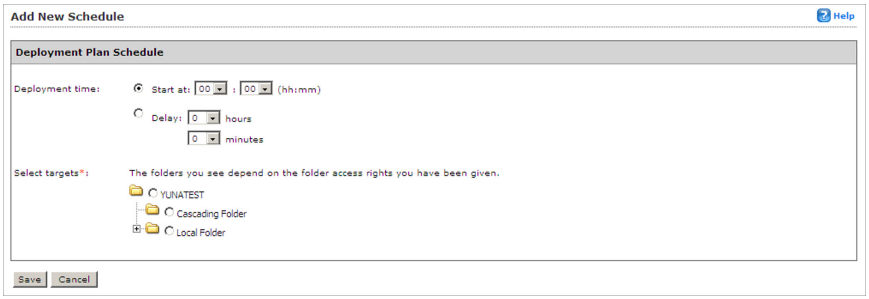
   Das Fenster **Add New Plan** wird angezeigt.



3. Geben Sie den Namen eines Verteilungsplans in das Feld **Name** ein.

4. Klicken Sie auf **Add**, um die Details zum Verteilungsplan anzugeben.

   Das Fenster **Add New Schedule** wird angezeigt.



5. Wählen Sie mit einer der folgenden Optionen im Fenster **Add New Schedule** einen Zeitplan für die Verteilung aus:

   - **Start at**: Führt die Verteilung zu einem bestimmten Zeitpunkt aus.

     Geben Sie in den Menüs den Zeitpunkt in Stunden und Minuten an.

   - **Delay**: Nach dem Download der aktuellen Komponenten verzögert Control Manager die Verteilung entsprechend dem von Ihnen angegebenen Intervall.

     Geben Sie in den Menüs die Dauer in Stunden und Minuten an.

6. Wählen Sie im Produktverzeichnis den Ordner, auf den der Zeitplan angewendet werden soll. Control Manager weist den Zeitplan allen Produkten zu, die sich in dem ausgewählten Ordner befinden.

7. Klicken Sie auf **Save**.

   Das Fenster **Add New Plan** wird angezeigt.

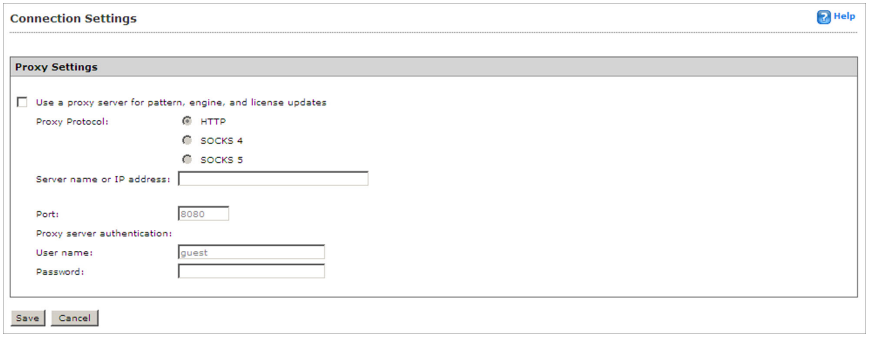
8. Klicken Sie auf **Save**, um den neuen Verteilungsplan zu übernehmen.

Schritt 2: Konfigurieren Sie die Proxy-Einstellungen (wenn Sie einen Proxy-Server verwenden).

Prozedur

1. Navigieren Sie zu **Administration** > **Settings** > **Proxy Settings**.

   Das Fenster **Connection Settings** wird angezeigt.



2. Wählen Sie **Use a proxy server for pattern, engine, and license updates** aus.
3. Wählen Sie das Protokoll:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Geben Sie den Host-Namen oder die IP-Adresse des Servers in das Eingabefeld **Server name or IP address** ein.
5. Geben Sie eine Portnummer in das Eingabefeld **Port** ein.

6. Geben Sie einen Anmeldenamen und ein Kennwort ein, wenn Ihr Server eine Authentifizierung erfordert.

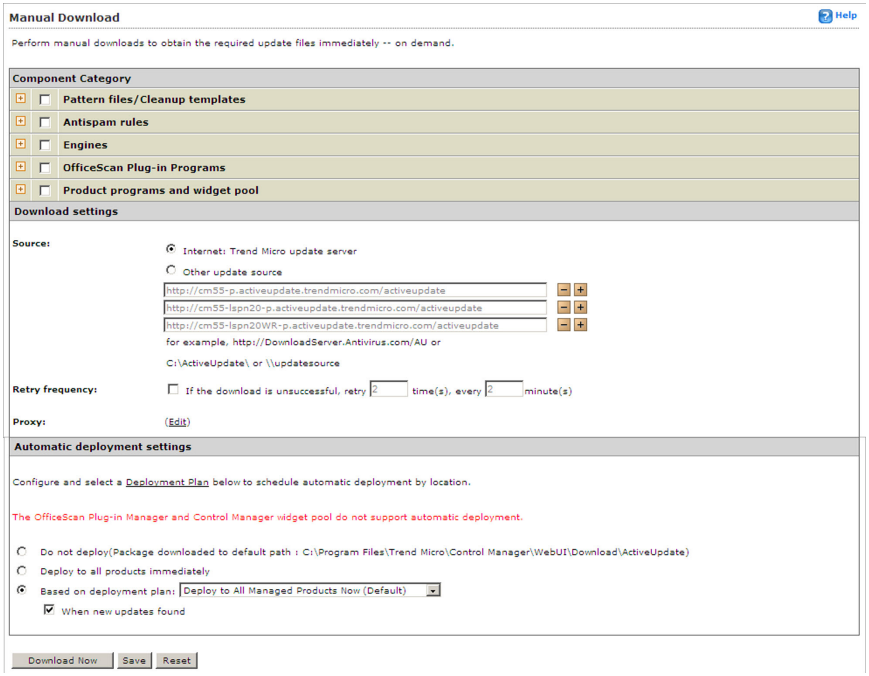
7. Klicken Sie auf **Save**.

Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.

Prozedur

1. Navigieren Sie zu **Updates** > **Manual Download**.

   Das Fenster **Manual Download** wird angezeigt.


Manual Download
Help
Perform manual downloads to obtain the required update files immediately -- on demand.
Component Category
Pattern files/Cleanup templates
Antispam rules
Engines
OfficeScan Plug-in Programs
Product programs and widget pool
Download settings
Source:
Internet: Trend Micro update server
Other update source
http://cm55-p.activeupdate.trendmicro.com/activeupdate
http://cm55-lspn20-p.activeupdate.trendmicro.com/activeupdate
http://cm55-lspn20WR-p.activeupdate.trendmicro.com/activeupdate
for example, http://DownloadServer.Antivirus.com/AU or
C:\ActiveUpdate\ or \\updatesource
Retry frequency:
If the download is unsuccessful, retry 2 time(s), every 2 minute(s)
Proxy:
(Edit)
Automatic deployment settings
Configure and select a Deployment Plan below to schedule automatic deployment by location.
The OfficeScan Plug-in Manager and Control Manager widget pool do not support automatic deployment.
Do not deploy(Package downloaded to default path : C:\Program Files\Trend Micro\Control Manager\WebUI\Download\ActiveUpdate)
Deploy to all products immediately
Based on deployment plan: Deploy to All Managed Products Now (Default)
When new updates found
Download Now
Save
Reset

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

a. Klicken Sie auf das +-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

- **Pattern files/Cleanup templates**
- **Antispam rules**
- **Engines**
- **OfficeScan Plug-in Programs**
- **Product programs and widget pool**

Schritt 4: Konfigurieren Sie die Download-Einstellungen.

Prozedur

1. Wählen Sie die Update-Adresse aus:

   - **Internet: Trend Micro update server**: Lädt die Komponenten vom offiziellen Trend Micro ActiveUpdate Server herunter.
   - **Other update source**: Geben Sie den URL der Update-Adresse in das zugehörige Eingabefeld ein.

     Unter **Other update source** können Sie mehrere Update-Adressen angeben. Klicken Sie auf das +-Symbol, um eine Update-Adresse hinzuzufügen. Sie können bis zu fünf Update-Adressen konfigurieren.

2. Wählen Sie **Retry frequency**, und geben Sie die Anzahl der Wiederholungen und die Dauer zwischen den Wiederholungen des Komponenten-Downloads an.

Tipp

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

3. Wenn Sie einen HTTP-Proxy-Server im Netzwerk verwenden (wenn der Control Manager Server keinen direkten Internet-Zugang hat), klicken Sie auf **Edit**, um die Proxy-Einstellungen im Fenster **Connection Settings** zu konfigurieren.

Schritt 5: Konfigurieren Sie die Einstellungen für die automatische Verteilung.

Prozedur

1. Wählen Sie im Bereich "Einstellungen für die automatische Verteilung" einen Verteilungszeitpunkt für die heruntergeladenen Komponenten aus. Wählen Sie zwischen:

   - **Do not deploy**: Die Komponenten werden auf den Control Manager heruntergeladen, aber nicht auf die verwalteten Produkte verteilt. Wählen Sie diese Option unter den folgenden Bedingungen:
     - Individuelle Verteilung auf die verwalteten Produkte
     - Die aktualisierten Komponenten werden vor der Verteilung getestet
   - **Deploy to all products immediately**: Die Komponenten werden auf den Control Manager heruntergeladen und dann auf die verwalteten Produkte verteilt.
   - **Based on deployment plan**: Die Komponenten werden auf den Control Manager heruntergeladen und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.
   - **When new updates found**: Die Komponenten werden auf den Control Manager heruntergeladen, wenn neue Komponenten unter der Update-Adresse verfügbar sind, und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.

Tipp

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

Schritt 6: Schließen Sie den manuellen Download ab.

Prozedur

1. Kicken Sie auf **Download Now** und bestätigen Sie mit **OK**.

   Das Download-Dialogfenster wird angezeigt. Die Fortschrittsanzeige zeigt den Download-Status an.

2. Klicken Sie auf **Command Details**, um weitere Einzelheiten im Fenster **Command Details** anzuzeigen.

3. Klicken Sie auf **OK**, um zum Fenster **Manual Download** zurückzukehren.

Grundlegendes zu Ausnahmen des zeitgesteuerten Downloads

Mit Hilfe von Download-Ausnahmen kann der Administrator verhindern, dass der Control Manager tagelang oder jeden Tag für eine bestimmte Zeit den Download von Trend Micro Update-Komponenten durchführt.

Diese Funktion ist besonders nützlich, wenn der Administrator die Komponenten-Downloads durch den Control Manager an einem arbeitsfreien Tag oder in der arbeitsfreien Zeit blockieren möchte.

Hinweis

Geplante tägliche Ausnahmen gelten für ausgewählte Tage, während geplante stündliche Ausnahmen für jeden Tag der Woche gelten.

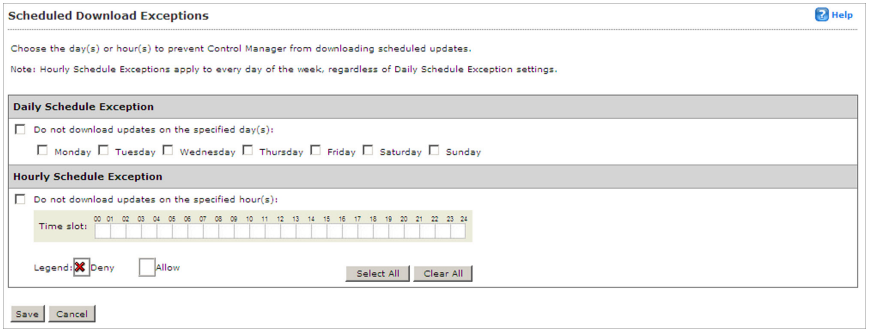
Beispiel: Der Administrator legt fest, dass Control Manager keine Komponenten an Wochenenden oder nach den Geschäftszeiten während der Woche herunterladen soll. Der Administrator aktiviert **Daily Schedule Exception** und wählt **Saturday** und **Sunday**. Der Administrator aktiviert anschließend **Hourly Schedule Exception** und gibt als Stunden **00:00 to 9:00** und **18:00 to 24:00** an.

Ausnahmen des zeitgesteuerten Downloads konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download Exceptions**.

   Das Fenster **Scheduled Download Exceptions** wird angezeigt.


Scheduled Download Exceptions
Help
Choose the day(s) or hour(s) to prevent Control Manager from downloading scheduled updates.
Note: Hourly Schedule Exceptions apply to every day of the week, regardless of Daily Schedule Exception settings.
Daily Schedule Exception
Do not download updates on the specified day(s):
Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Hourly Schedule Exception
Do not download updates on the specified hour(s):
Time slot:
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Legend: Deny Allow
Select All
Clear All
Save
Cancel

2. Wählen Sie mindestens eine der folgenden Einstellungen:

   - Zur Planung einer täglichen Ausnahme aktivieren Sie im Bereich "Ausnahmen vom Zeitplan (Tage)" einen oder mehrere Tage, an dem bzw. an denen keine Downloads durchgeführt werden, und wählen Sie anschließend **Do not download updates on the specified day(s)**. Jede Woche werden dadurch von Control Manager alle Downloads an den ausgewählten Tagen blockiert.

   - Zur Planung einer stündlichen Ausnahme aktivieren Sie im Bereich "Ausnahmen vom Zeitplan (Stunden)" eine oder mehrere Stunden, an der

bzw. an denen keine Downloads durchgeführt werden, und wählen Sie anschließend **Do not download updates on the specified hour(s)**. Jeden Tag werden dadurch von Control Manager alle Downloads zu den ausgewählten Stunden blockiert.

3. Klicken Sie auf **Save**.

Zeitgesteuerte Downloads konfigurieren

Konfigurieren Sie zeitgesteuerte Komponenten-Downloads, um Ihre Komponenten auf dem neuesten Stand zu halten und Ihr Netzwerk zu schützen. Control Manager unterstützt den Download einzelner Komponenten. Sie können Download-Zeitpläne sowohl für Komponentengruppen als auch für einzelne Komponenten angeben. Alle Zeitpläne sind voneinander unabhängig. Alle Komponenten einer Gruppe werden gemäß einem Download-Zeitplan für diese Komponentengruppe heruntergeladen.

Im Fenster **Scheduled Download** finden Sie folgende Informationen über aktuell in Ihrem Control Manager System vorhandene Komponenten:

- **Zeitintervall**: Zeigt an, wie oft die Komponente aktualisiert wird.
- **Aktiviert**: Zeigt an, ob der Zeitplan für die Komponente aktiviert oder deaktiviert ist.
- **Update-Adresse**: Zeigt den URL bzw. den Pfad der Update-Adresse an.

Die Konfiguration zeitgesteuerter Komponenten-Downloads erfordert mehrere Schritte:

- Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.
- Schritt 2: Konfigurieren Sie Ihre Proxy-Einstellungen, wenn Sie einen Proxy-Server verwenden.
- Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.
- Schritt 4: Konfigurieren Sie den Download-Zeitplan.
- Schritt 5: Konfigurieren Sie die Download-Einstellungen.
- Schritt 6: Konfigurieren Sie die Einstellungen für die automatische Verteilung.

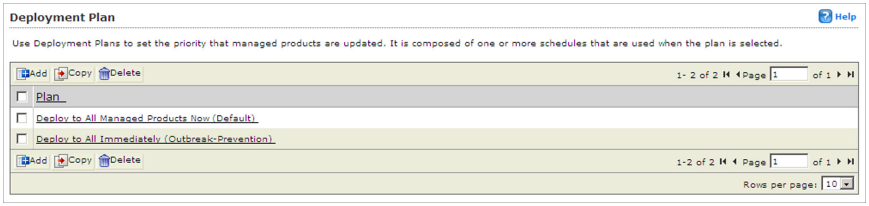
- Schritt 7: Aktivieren Sie den Zeitplan, und speichern Sie die Einstellungen.

Schritt 1: Konfigurieren Sie einen Verteilungsplan für Ihre Komponenten.

Prozedur

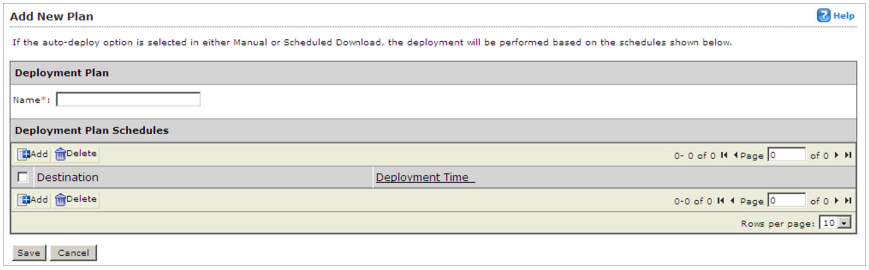
1. Navigieren Sie zu **Updates** > **Deployment Plan**.

   Das Fenster **Deployment Plan** wird angezeigt.



2. Klicken Sie auf **Add**.

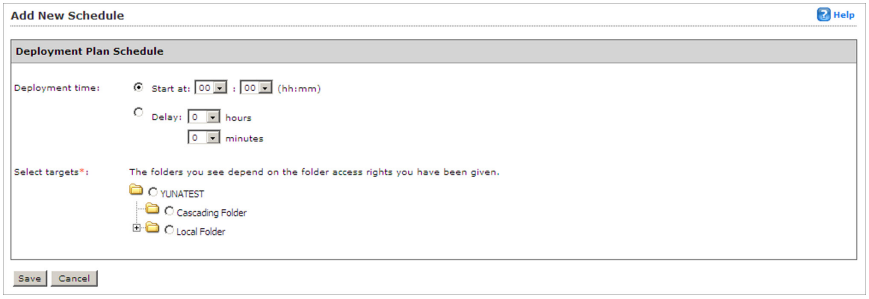
   Das Fenster **Add New Plan** wird angezeigt.



3. Geben Sie den Namen eines Verteilungsplans in das Feld **Name** ein.

4. Klicken Sie auf **Add**, um die Details zum Verteilungsplan anzugeben.

   Das Fenster **Add New Schedule** wird angezeigt.



5. Wählen Sie einen Verteilungszeitplan, indem Sie eine der folgenden Optionen auswählen:

   - **Start at**: Führt die Verteilung zu einem bestimmten Zeitpunkt aus.

     Geben Sie in den Menüs den Zeitpunkt in Stunden und Minuten an.

   - **Delay**: Nach dem Download der aktuellen Komponenten verzögert Control Manager die Verteilung entsprechend dem von Ihnen angegebenen Intervall.

     Geben Sie in den Menüs die Dauer in Stunden und Minuten an.

6. Wählen Sie im Produktverzeichnis den Ordner, auf den der Zeitplan angewendet werden soll. Control Manager weist den Zeitplan allen Produkten zu, die sich in dem ausgewählten Ordner befinden.

7. Klicken Sie auf **Save**.

   Das Fenster **Add New Plan** wird angezeigt.

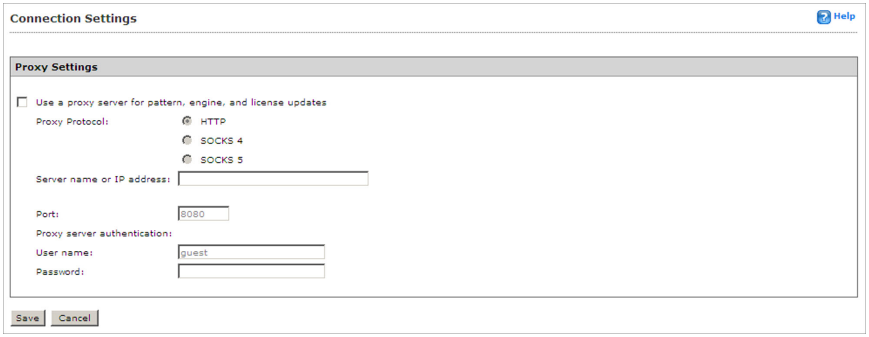
8. Klicken Sie auf **Save**, um den neuen Verteilungsplan zu übernehmen.

Schritt 2: Konfigurieren Sie die Proxy-Einstellungen (wenn Sie einen Proxy-Server verwenden).

Prozedur

1. Navigieren Sie zu **Administration** > **Settings** > **Proxy Settings**.

   Das Fenster **Connection Settings** wird angezeigt.



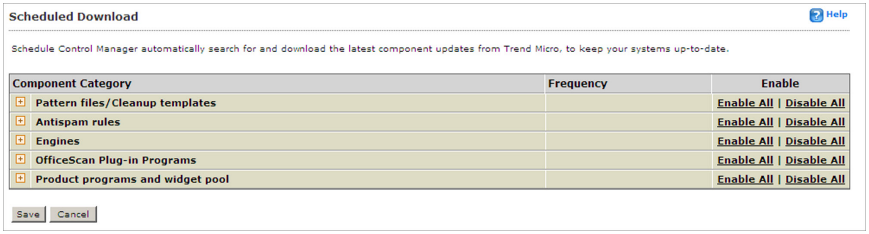
2. Wählen Sie **Use a proxy server for pattern, engine, and license updates** aus.
3. Wählen Sie das Protokoll:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Geben Sie den Host-Namen oder die IP-Adresse des Servers in das Eingabefeld **Server name or IP** ein.
5. Geben Sie eine Portnummer für den Proxy-Server in das Feld **Port** ein.
6. Geben Sie einen Anmeldenamen und ein Kennwort ein, wenn Ihr Server eine Authentifizierung erfordert.
7. Klicken Sie auf **Save**.

Schritt 3: Wählen Sie die zu aktualisierenden Komponenten.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.



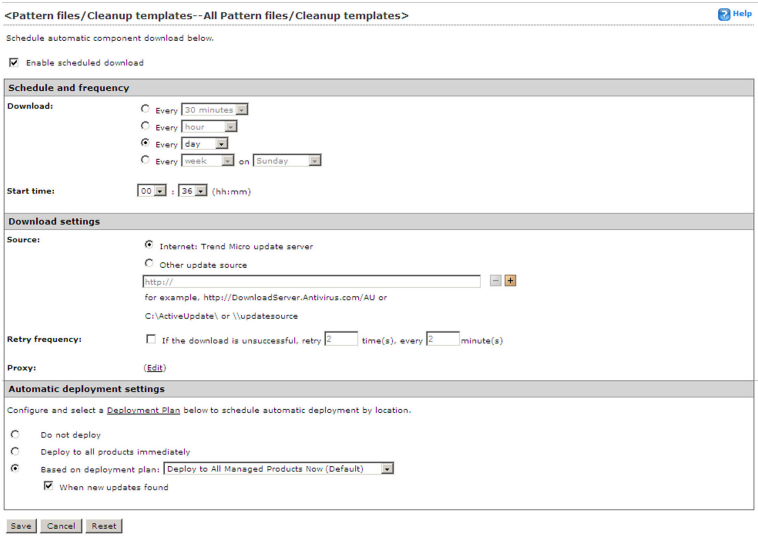
2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

- **All Pattern files/Cleanup templates**
- **All Antispam rules**
- **All Engines**
- **OfficeScan Plug-in Programs**
- **Product programs and widget pool**

Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.



Schritt 4: Konfigurieren Sie den Download-Zeitplan.

Prozedur

1. Aktivieren Sie das Kontrollkästchen **Enable scheduled download**, um den zeitgesteuerten Komponenten-Download zu aktivieren.
2. Legen Sie den Download-Zeitplan fest. Wählen Sie ein Intervall aus, und verwenden Sie zur Angabe des gewünschten Zeitplans das entsprechende Listenfeld. Sie können einen Download nach Minuten, Stunden, Tagen oder Wochen planen.
3. Mit dem Menü **Start time** geben Sie an, an welchem Datum und zu welcher Uhrzeit der Zeitplan wirksam wird.

Schritt 5: Konfigurieren Sie die Download-Einstellungen.

Prozedur

1. Wählen Sie die Update-Adresse aus:

   - **Internet**: **Trend Micro update server**: Lädt die Komponenten vom offiziellen Trend Micro ActiveUpdate Server herunter.
   - **Other update source**: Geben Sie den URL der Update-Adresse in das zugehörige Eingabefeld ein.

     Unter **Other update source** können Sie mehrere Update-Adressen angeben. Klicken Sie auf das **+**-Symbol, um eine Update-Adresse hinzuzufügen. Sie können bis zu fünf Update-Adressen konfigurieren.

2. Wählen Sie **Retry frequency**, und geben Sie die Anzahl der Wiederholungen und die Dauer zwischen den Wiederholungen des Komponenten-Downloads an.

   Hinweis

   Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

3. Wenn Sie einen HTTP-Proxy-Server im Netzwerk verwenden (wenn der Control Manager Server keinen direkten Internet-Zugang hat), klicken Sie auf **Edit**, um die Proxy-Einstellungen im Fenster **Connection Settings** zu konfigurieren.

Schritt 6: Konfigurieren Sie die Einstellungen für die automatische Verteilung.

Prozedur

1. Wählen Sie im Bereich "Einstellungen für die automatische Verteilung" einen Verteilungszeitpunkt für die heruntergeladenen Komponenten aus. Wählen Sie zwischen:

- **Do not deploy**: Die Komponenten werden auf den Control Manager heruntergeladen, aber nicht auf die verwalteten Produkte verteilt. Wählen Sie diese Option unter den folgenden Bedingungen:
  - Individuelle Verteilung auf die verwalteten Produkte
  - Die aktualisierten Komponenten werden vor der Verteilung getestet
- **Deploy immediately**: Die Komponenten werden auf Control Manager heruntergeladen und dann auf die verwalteten Produkte verteilt.
- **Based on deployment plan**: Die Komponenten werden auf den Control Manager heruntergeladen und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.
- **When new updates found**: Wenn neue Komponenten unter der Update-Adresse verfügbar sind, werden die Komponenten auf den Control Manager heruntergeladen und an die verwalteten Produkte verteilt.

Hinweis

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

2. Wählen Sie im Fenster **Deployment Plan** einen Verteilungsplan, nachdem die Komponenten auf Control Manager heruntergeladen wurden.
3. Klicken Sie auf **Save**.

Schritt 7: Aktivieren Sie den Zeitplan, und speichern Sie die Einstellungen.

Prozedur

1. Klicken Sie auf die Schaltfläche "Status" in der Spalte **Enable**.
2. Klicken Sie auf **Save**.

Zeitplan und Häufigkeit für zeitgesteuerte Downloads konfigurieren

Sie können in der Gruppe "Zeitplan und Häufigkeit" angeben, wie oft Control Manager Komponenten-Updates abruft.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.

3. Unter Zeitplan und Häufigkeit:

   a. Legen Sie den Download-Zeitplan fest. Wählen Sie ein Intervall aus, und verwenden Sie zur Angabe des gewünschten Zeitplans das entsprechende Listenfeld. Sie können einen Download nach Minuten, Stunden, Tagen oder Wochen planen.

b. Im Dropdown-Menü **Start time** legen Sie das Datum und die Uhrzeit fest, wann der Zeitplan wirksam wird.

4. Klicken Sie auf **Save**.

Einstellungen für zeitgesteuerte Downloads konfigurieren

In der Gruppe "Download-Einstellungen" können Sie die Komponenten definieren, die Control Manager automatisch herunterlädt, sowie die Download-Methode.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.

3. Wählen Sie unter "Download-Einstellungen" eine der folgenden Update-Adressen:

- **Internet: Trend Micro update server**: (Standardeinstellung) Control Manager lädt die neuesten Komponenten vom Trend Micro ActiveUpdate Server herunter.
- **Other update source**: Ermöglicht die Angabe eines URL für den Speicherort der neuesten Komponentenversion, z. B. der Intranet-Server Ihres Unternehmens.

  Unter **Other update source** können Sie mehrere Update-Adressen angeben. Klicken Sie auf das +-Symbol, um eine zusätzliche Update-Adresse hinzuzufügen. Sie können bis zu fünf Update-Adressen konfigurieren.

4. Wählen Sie **Retry frequency**, um Control Manager anzuweisen, den Download der neuesten Komponenten erneut zu versuchen. In den entsprechenden Feldern können Sie die Anzahl der Versuche und das Intervall zwischen den Versuchen eingeben.

Hinweis

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

5. Wenn Sie einen HTTP-Proxy-Server im Netzwerk verwenden (wenn der Control Manager Server keinen direkten Internet-Zugang hat), klicken Sie auf **Edit**, um die Proxy-Einstellungen im Fenster **Connection Settings** zu konfigurieren.
6. Klicken Sie auf **Save**.

Automatische Verteilungseinstellungen für den zeitgesteuerten Download konfigurieren

In der Gruppe für die automatischen Verteilungseinstellungen können Sie festlegen, wie Control Manager Aktualisierungen verteilt.

Prozedur

1. Navigieren Sie zu **Updates** > **Scheduled Download**.

   Das Fenster **Scheduled Download** wird angezeigt.

2. Wählen Sie im Bereich "Komponentenkategorie" die Download-Komponenten aus.

   a. Klicken Sie auf das **+**-Symbol, um die Komponentenliste für jede Komponentengruppe anzuzeigen.

   b. Wählen Sie die gewünschten Komponenten aus. Um alle Komponenten für eine Gruppe auszuwählen, wählen Sie:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        Das Fenster <Komponentenname> wird angezeigt. <Komponentenname> steht für den Namen der ausgewählten Komponente.

3. Wählen Sie im Bereich "Einstellungen für die automatische Verteilung" einen Verteilungszeitpunkt für die heruntergeladenen Komponenten aus. Wählen Sie zwischen:

   - **Do not deploy**: Die Komponenten werden auf den Control Manager heruntergeladen, aber nicht auf die verwalteten Produkte verteilt. Wählen Sie diese Option unter den folgenden Bedingungen:
     - Individuelle Verteilung auf die verwalteten Produkte
     - Die aktualisierten Komponenten werden vor der Verteilung getestet
   - **Deploy immediately**: Die Komponenten werden auf Control Manager heruntergeladen und dann auf die verwalteten Produkte verteilt.
   - **Based on deployment plan**: Die Komponenten werden auf den Control Manager heruntergeladen und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.
   - **When new updates found**: Die Komponenten werden auf den Control Manager heruntergeladen, wenn neue Komponenten unter der Update-

Adresse verfügbar sind, und anhand eines von Ihnen gewählten Zeitplans auf die verwalteten Produkte verteilt.

Hinweis

Klicken Sie auf **Save** und anschließend in diesem Fenster auf **Edit** oder **Deployment Plan**. Ihre Einstellungen werden nur übernommen, wenn Sie auf **Save** klicken.

4. Wählen Sie im Fenster **Deployment Plan** einen Verteilungsplan, nachdem die Komponenten auf Control Manager heruntergeladen wurden.

5. Klicken Sie auf **Save**.

Hinweis

Die Einstellungen in der Gruppe der automatischen Verteilungseinstellungen gelten nur für Komponenten, die von verwalteten Produkte verwendet werden.

Grundlegendes zu Verteilungsplänen

Mit einem Verteilungsplan können Sie die Reihenfolge festlegen, in der Control Manager Ihre Gruppen von verwalteten Produkten aktualisiert. Mit Control Manager können Sie mehrere Verteilungspläne für unterschiedliche verwaltete Produkte implementieren, die jeweils unterschiedliche Zeitpläne haben. So können Sie beispielsweise während eines Ausbruchs im Zusammenhang mit einem E-Mail-Virus der Aktualisierung der Software-Komponenten für das Durchsuchen von E-Mail-Nachrichten eine höhere Priorität zuweisen, z. B. der letzten Viren-Pattern-Datei für Trend Micro ScanMail für Microsoft Exchange.

Die Control Manager Installation erstellt zwei Verteilungspläne:

- Jetzt an alle verwalteten Produkte verteilen (Standard): Standardplan, der während der Komponenten-Updates verwendet wird
- An alle unverzüglich verteilen (Outbreak-Prevention): Standardplan für die Präventionsphase von Outbreak Prevention Services

Standardmäßig werden auf Grundlage dieser Pläne Updates sofort auf alle Produkte im Produktverzeichnis verteilt.

Wählen Sie oder erstellen Sie Pläne in den Fenstern "Manueller Download" und "Zeitgesteuerter Download". Sie können diese Pläne anpassen oder – entsprechend den Anforderungen in Ihrem Netzwerk – neue erstellen. Erstellen Sie z. B. Verteilungspläne entsprechend der Natur des Ausbruchs:

- E-Mail-Virus
- File-Sharing-Virus

Die Verteilung von Updates an das Produktverzeichnis erfolgt getrennt vom Download-Prozess.

Control Manager lädt die Komponenten herunter und folgt dem Verteilungsplan entsprechend den Einstellungen für manuelle oder zeitgesteuerte Downloads.

Beachten Sie die folgenden Punkte, wenn Sie einen Verteilungsplan erstellen oder implementieren:

- Sie können Verteilungszeitpläne Ordnern, jedoch nicht spezifischen Produkten zuweisen.

  Aus diesem Grund ist die Planung des Inhalts der Produktverzeichnisordner besonders wichtig.

- Sie können nur jeweils einen Ordner für einen Verteilungsplan-Zeitplan festlegen.

  Sie können jedoch mehr als einen Zeitplan pro Verteilungsplan festlegen.

- Control Manager legt die Verzögerungen des Verteilungsplans abhängig von der Ausführungszeit des Downloads fest, und diese Verzögerungen sind unabhängig voneinander.

  Wenn Sie beispielsweise drei Ordner haben, die in Intervallen von 5 Minuten aktualisiert werden sollen, können Sie dem ersten Ordner eine Verzögerung von 5 Minuten zuweisen und anschließend Verzögerungen von 10 und 15 Minuten für die beiden verbleibenden Ordner festlegen.

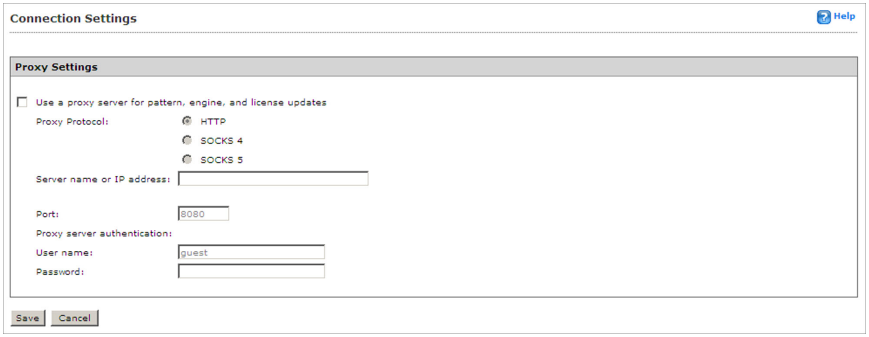
Proxy-Einstellungen konfigurieren

Sie können die Verbindung mit einem Proxy-Server für Komponenten-Downloads und Lizenzaktualisierungen konfigurieren.

Prozedur

1. Navigieren Sie zu **Administration** > **Settings** > **Proxy Settings**.

   Das Fenster **Connection Settings** wird angezeigt.



2. Wählen Sie **Use a proxy server for pattern, engine, and license updates** aus.
3. Wählen Sie das Protokoll:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Geben Sie den Host-Namen oder die IP-Adresse des Servers in das Eingabefeld **Server name or IP address** ein.
5. Geben Sie eine Portnummer in das Eingabefeld **Port** ein.
6. Geben Sie einen Anmeldenamen und ein Kennwort ein, wenn Ihr Server eine Authentifizierung erfordert.
7. Klicken Sie auf **Save**.

Aktualisierungs-/Verteilungseinstellungen konfigurieren

Die Verwendung von HTTPS zum Herunterladen von Komponenten vom Trend Micro ActiveUpdate Server (der Standard-Download-Adresse) oder einer anderen Update-Adresse ist eine sicherere Methoden für das Abrufen von Komponenten.

Wenn Komponenten aus einem Freigabeordner in einem Netzwerk heruntergeladen werden, müssen Sie die Authentifizierung für das lokale Windows-Konto und Remote UNC festlegen.

Die lokale Windows-Authentifizierung verweist auf das Active Directory-Benutzerkonto auf dem Control Manager Server. Das Konto sollte über Folgendes verfügen:

- Administratorberechtigung
- Richtlinie *Anmelden als Stapelverarbeitungsauftrag* festgelegt

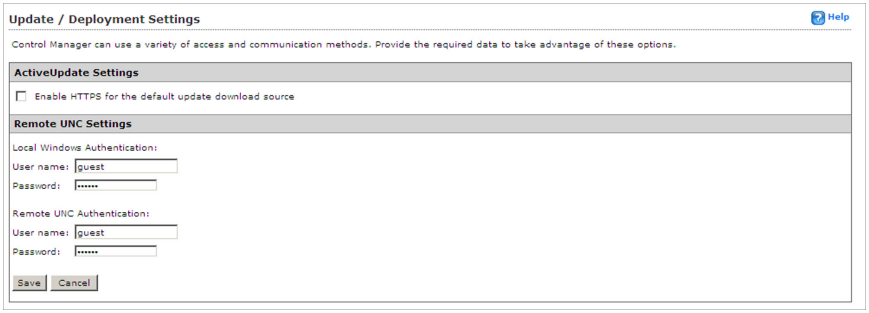
Die Funktion **UNC-Remote-Authentifizierung** verwendet ein Benutzerkonto vom Komponentenquellen-Server mit der Berechtigung, einen Ordner freizugeben, in den Control Manager die Updates herunterladen wird.

HTTPS-Download aktivieren

Prozedur

1. Navigieren Sie zu **Updates** > **Update/Deployment Settings**.

   Das Fenster **Update/Deployment Settings** wird angezeigt.



2. Wählen Sie **Enable HTTPS for the default update download source**.
3. Klicken Sie auf **Save**.
4. Navigieren Sie zum Fenster **Manual Download** oder **Scheduled Download**.
5. Wählen Sie im Arbeitsbereich unter **Download settings Internet: Trend Micro update server**, oder geben Sie den Komponentenquellen-Server Ihres Unternehmens in das Feld **Other update source** ein.
6. Klicken Sie auf **Save**.

UNC-Download aktivieren

Prozedur

1. Navigieren Sie zu **Updates** > **Update/Deployment Settings**.

   Das Fenster **Update/Deployment Settings** wird angezeigt.
2. Geben Sie die Benutzernamen und Kennwörter für die **Local Windows Authentication** und die **Remote UNC Authentication** ein.
3. Klicken Sie auf **Save**.
4. Navigieren Sie zum Fenster **Manual Download** oder **Scheduled Download**.
5. Wählen Sie im Arbeitsbereich unter **Download settings** die Option **Other update source** aus, und geben Sie anschließend einen freigegebenen Netzwerkordner ein.
6. Klicken Sie auf **Save**.

Richtlinie "Anmelden als Stapelverarbeitungsauftrag" einrichten

Die lokale Windows-Authentifizierung verweist auf das Active Directory-Benutzerkonto auf dem Control Manager Server. Das Konto sollte über Folgendes verfügen:

- Administratorberechtigung

- Richtlinie "Anmelden als Stapelverarbeitungsauftrag" festgelegt

---

Prozedur

1. Klicken Sie auf **Start** > **Settings** > **Control Panel**.
2. Klicken Sie auf **Administrative Tools**.
3. Öffnen Sie **Local Security Policy**. Das Fenster "Lokale Sicherheitseinstellungen" wird angezeigt.
4. Klicken Sie auf **Local Polices** > **User Rights Assignment**.
5. Doppelklicken Sie auf **Log on as a batch job**.

   Das Dialogfeld **Log on as a batch job Properties** wird angezeigt.
6. Fügen Sie den Benutzer hinzu, wenn dieser nicht in der Liste angezeigt wird.

Protokolle verwenden

Auch wenn Control Manager Daten von mehreren Protokolltypen empfängt, ermöglicht Control Manager, dass Benutzer Protokolldaten direkt aus der Control Manager Datenbank abrufen. Benutzer können anschließend Filterkriterien angeben, um nur die Daten zusammenzustellen, die sie benötigen.

Control Manager unterstützt auch die Protokollzusammenführung. Die Protokollzusammenführung kann die Abfrageleistung verbessern und die Netzwerkbandbreite reduzieren, die verwaltete Produkte beim Senden von Protokollen an Control Manager benötigen. Dies geschieht jedoch auf Kosten von Daten, die durch die Zusammenführung verloren gehen. Control Manager kann keine Daten abfragen, die in der Control Manager Datenbank nicht vorhanden sind.

Grundlegendes zu Protokollen von verwalteten Produkten

Protokolle von verwalteten Produkten enthalten Informationen über die Leistung der verwalteten Produkte. Sie können Informationen zu bestimmten Produkten oder

Gruppen von Produkten abrufen, die vom übergeordneten oder untergeordneten Server verwaltet werden. Mit der von Control Manager unterstützen Datenabfrage zu Protokollen und den Funktionen zur Datenfilterung können sich Administratoren auf die Informationen konzentrieren, die sie benötigen.

Hinweis

Mehr Protokolle bedeuten reichliche Informationen über das Control Manager Netzwerk. Diese Protokolle belegen jedoch Speicherplatz. Es ist Ihre Aufgabe, einen Ausgleich zwischen dem Bedarf an Informationen und den verfügbaren Systemressourcen zu finden.

Abhängig von ihrer Funktion generieren verwaltete Produkte verschiedene Arten von Protokollen.

TABELLE A-11. Protokolle von verwalteten Produkten

PROTOKOLLKATEGORIE	BESCHREIBUNG
Produktinformationen	Protokolle zu Produktinformationen enthalten Informationen zu Themen wie dem Benutzerzugriff und Ereignissen bei verwalteten Produkte bis hin zur Verteilung von Komponenten und dem Aktualisierungsstatus. • Informationen zu verwalteten Produkten • Versionsinformationen

PROTOKOLLKATEGORIE	BESCHREIBUNG
Informationen zu Sicherheitsbedrohungen	Protokolle zu Sicherheitsbedrohungen enthalten Informationen zu bekannten und potenziellen Sicherheitsbedrohungen, die in Ihrem Netzwerk erkannt wurden. • Viren-/Malware-Informationen • Spyware-/Grayware-Informationen • Informationen zu Content-Verstößen • Informationen zu Spam-Verstößen • Informationen Richtlinien-/Regelverstößen • Informationen zu Web-Verstößen/-Reputation • Informationen zu verdächtigen Bedrohungen • Allgemeine Informationen zu Bedrohungen
Informationen zun Datenschutz	Die Datenschutz-Protokolle enthalten Informationen zu DLP-Vorfällen, Vorlagenübereinstimmungen und Quellen für Vorfälle. • Informationen zur Prävention vor Datenverlust

Protokolldaten abfragen

Ad-hoc-Abfragen bieten Administratoren eine schnelle Methode, um Informationen direkt aus der Control Manager Datenbank abzurufen. Die Datenbank enthält alle Informationen, die von allen Produkten gesammelt wurden, die bei Control Manager Server registriert sind (Protokollzusammenführung kann sich auf die Datenverfügbarkeit der Abfrage auswirken). Ad-hoc-Abfragen stellen ein sehr leistungsfähiges Tool für Administratoren bereit.

Bei der Abfrage von Daten können Administratoren die Abfragekriterien filtern, so dass nur die benötigten Daten zurückgegeben werden. Administratoren können anschließend die Daten zur weiteren Analyse in das CSV- oder XML-Format exportieren oder die Abfrage zur zukünftigen Verwendung speichern. Control Manager unterstützt auch die Freigabe von gespeicherten Abfragen für andere Benutzer, so dass diese von nützlichen Abfragen profitieren.

Füllen Sie die Ad-hoc-Abfrage wie folgt aus:

- Schritt 1: Wählen Sie das verwaltete Produkt oder den aktuellen Control Manager Server für die Abfrage.
- Schritt 2: Wählen Sie die Datenansicht, die abgefragt werden soll.
- Schritt 3: Geben Sie die Filterkriterien sowie die spezifischen Informationen an, die angezeigt werden sollen.
- Schritt 4: Speichern Sie die Abfrage, und führen Sie sie aus.
- Schritt 5: Exportieren Sie die Daten in einer .CSV- oder .XML-Datei.

Hinweis

Control Manager unterstützt die Freigabe von gespeicherten Ad-hoc-Abfragen für andere Benutzer. Gespeicherte und freigegebene Abfragen werden im Fenster **Saved Ad Hoc Queries** angezeigt.

Grundlegendes zu Datenansichten

Bei einer Datenansicht handelt es sich um eine Tabelle, die aus Gruppen verwandter Datenzellen besteht. Datenansichten stellen die Grundlage dar, auf der Benutzer Ad-hoc-Abfragen an die Control Manager Datenbank stellen.

Control Manager ermöglicht direkte Abfragen der Control Manager Datenbank. Datenansichten sind für Berichtvorlagen vom Typ Control Manager 5 und für Ad-hoc-Abfragen verfügbar.

Datenansichten sind Tabellen, die mit Informationen gefüllt sind. Jede Überschrift in einer Datenansicht dient als Spalte in einer Tabelle. Die Dateiansicht "Viren/Malware Aktion/Ergebnis-Zusammenfassung" enthält beispielsweise die folgenden Überschriften:

- Aktionsergebnis
- Durchgeführte Aktion
- Eindeutige Endpunkte
- Eindeutige Quellen

- Funde

Als Tabelle nimmt die Datenansicht das folgende Format mit potenziellen Unterüberschriften unter jeder Überschrift an:

TABELLE A-12. Beispieldatenansicht

AKTIONSERGEBNIS	DURCHGEFÜHRTE AKTION	EINDEUTIGE ENDPUNKTE	EINDEUTIGE QUELLEN	FUNDE

Es ist wichtig, dass Sie sich an diese Informationen erinnern, wenn Sie festlegen, wie Daten in einer Berichtvorlage angezeigt werden.

Control Manager trennt Datenansichten in zwei Hauptkategorien: Produktinformationen und Informationen zu Sicherheitsbedrohungen. Weitere Informationen zu Datenansichten finden Sie im Anhang. Die Hauptkategorien sind ferner in mehrere Unterkategorien unterteilt. Dabei sind die Unterkategorien in zusammenfassende Informationen und detaillierte Informationen unterteilt.

Grundlegendes zu Berichten

Control Manager Berichte bestehen aus zwei Teilen: Berichtvorlagen und Berichtprofile. Während eine Berichtvorlage das Erscheinungsbild des Berichts bestimmt, werden im Berichtprofil der Ursprung der Berichtdaten, der Zeitplan bzw. das Zeitintervall und die Empfänger des Berichts angegeben.

Im Vergleich zu früheren Control Manager Versionen wurden in Control Manager 5.0 radikale Änderungen durch die Einführung angepasster Berichte für Control Manager Administratoren integriert. Control Manager 6.0 unterstützt weiterhin Berichtvorlagen aus früheren Control Manager Versionen, jedoch können Administratoren mit Control Manager 6.0 ihre eigenen angepassten Berichtvorlagen entwickeln.

Grundlegendes zu Control Manager Berichtvorlagen

Eine Berichtvorlage beschreibt das Aussehen des Control Manager Berichtes. Control Manager unterteilt Berichtvorlagen in folgende Typen:

- Control Manager 5 Vorlagen: Benutzerdefinierte Berichtvorlagen, in denen direkte Datenbankabfragen (Datenbankansichten) und Elemente von Berichtvorlagen (Diagramme und Tabellen) verwendet werden. Im Vergleich zu früheren Control Manager Versionen erhalten Benutzer mehr Flexibilität bei der Angabe der Daten, die ihn den Berichten angezeigt werden. Weitere Informationen zu Control Manager 5 Vorlagen finden Sie unter *Grundlegendes zu Vorlagen für Control Manager 5 auf Seite A-75*.

- Control Manager 3 Vorlagen: Enthalten vordefinierte Vorlagen. Weitere Informationen zu Control Manager 3 Vorlagen finden Sie unter *Grundlegendes zu Vorlagen für Control Manager 3 auf Seite A-82*.

Grundlegendes zu Vorlagen für Control Manager 5

Control Manager 5 Berichtvorlagen verwenden Datenbankansichten als Informationsgrundlage für Berichte. Weitere Informationen zu Datenansichten finden Sie unter *Grundlegendes zu Datenansichten auf Seite A-73*. Das Erscheinungsbild der generierten Berichte hängt von den Berichtelementen ab. Berichtelemente bestehen aus dem Folgenden.

TABELLE A-13. Elemente der Control Manager 5 Berichtvorlagen

VORLAGENELEMENT	BESCHREIBUNG
Seitenumbruch	Fügt einen Seitenumbruch in einen Bericht ein. Jede Berichtseite unterstützt bis zu drei Berichtvorlagenelemente.
Statischer Text	Bietet Platz für eine benutzerdefinierte Beschreibung oder Erklärung zum Bericht. Der Inhalt des statischen Textes kann bis zu 4096 Zeichen lang sein.
Balkendiagramm	Fügt ein Balkendiagramm in eine Berichtvorlage ein.
Liniendiagramm	Fügt ein Liniendiagramm in eine Berichtvorlage ein.
Kreisdiagramm	Fügt ein Kreisdiagramm in eine Berichtvorlage ein.
Dynamische Tabelle	Fügt eine dynamische/Kreuztabelle in eine Berichtvorlage ein.
Rastertabelle	Fügt ein Tabelle in eine Berichtvorlage ein. In einer Rastertabelle werden dieselben Informationen angezeigt wie in einer Ad-hoc-Abfrage.

Jede Control Manager 5 Vorlage kann bis zu 100 Berichtvorlagenelemente enthalten. Auf jeder Seite in der Berichtvorlage können sich bis zu drei Berichtvorlagenelemente befinden. Mit Seitenumbrüchen fügen Sie Seiten zu einer Berichtvorlage hinzu.

Damit Sie die Control Manager 5 Berichtvorlagen besser verstehen, stellt Trend Micro die folgenden vordefinierten Berichtvorlagen bereit.

Hinweis

Öffnen Sie das Fenster **Report Templates**, um die vordefinierten Vorlagen von Trend Micro anzuzeigen.

TABELLE A-14. Vordefinierte Control Manager 5 Vorlagen

VORLAGE	BESCHREIBUNG
Zusammenfassung zu erkannten TM-Content-Verstößen	Stellt die folgenden Informationen bereit: • Erkannte Content-Verstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Richtlinienverstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl Absender/Benutzer-Verstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigsten Richtlinien mit Verstößen (Balkendiagramm) • Zusammenfassung zu Content-Verstößen - Richtlinie (Rastertabelle) • Die 25 häufigsten Absender/Benutzer mit Verstößen (Balkendiagramm) • Zusammenfassung Content-Verstöße – Absender/ Benutzer mit Verstößen (Rastertabelle) • Zusammenfassung zu Aktionsergebnissen (Kreisdiagramm)

VORLAGE	BESCHREIBUNG
TM – Status der Verbindung/ Komponenten von verwalteten Produkten	Stellt die folgenden Informationen bereit: • Verbindungsstatus Server/Appliance (Kreisdiagramm) • Verbindungsstatus Client (Kreisdiagramm) • Aktualisierungsstatus Server/Appliance-Pattern-Datei/ Regel (Kreisdiagramm) • Aktualisierungsstatus Client-Pattern-Datei/Regel (Kreisdiagramm) • Aktualisierungsstatus Server/Appliance Scan Engine (Kreisdiagramm) • Aktualisierungsstatus Client Scan Engine (Kreisdiagramm) • Pattern-Datei/Regel-Zusammenfassung für Server/ Appliances (Rastertabelle) • Pattern-Datei/Regel-Zusammenfassung für Clients (Rastertabelle) • Scan Engine-Zusammenfassung für Server/Appliances (Rastertabelle) • Scan Engine-Zusammenfassung für Clients (Rastertabelle)
TM - Allgemeine Zusammenfassung zu Bedrohungen	Stellt die folgenden Informationen bereit: • Zusammenfassung zur vollständigen Risikoanalyse der Netzwerksicherheit (Rastertabelle) • Zusammenfassung Netzwerkschutzgrenze (Rastertabelle) • Informationen zur Analyse von Sicherheitsrisiken für Endpunkte (Rastertabelle) • Informationen zur Analyse von Sicherheitsrisiken für Ziele (Rastertabelle) • Informationen zur Analyse von Sicherheitsrisiken für Quellen (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Spam-Erkennung	Stellt die folgenden Informationen bereit: • Spam-Erkennung, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger-Domänen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger, gruppiert nach Tag (Liniendiagramm) • Die häufigsten 25 Empfänger-Domänen (Balkendiagramm) • Allgemeine Zusammenfassung zu Spam-Verstößen (Rastertabelle) • Die häufigsten 25 Empfänger von Spam (Balkendiagramm) • Zusammenfassung zu Spam-Empfängern (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Spyware/Grayware-Erkennung	Stellt die folgenden Informationen bereit: • Spyware/Grayware-Erkennung, gruppiert nach Tag (Liniendiagramm) • Anzahl eindeutiger Spyware/Grayware, gruppiert nach Tag (Liniendiagramm) • Anzahl Spyware/Grayware-Quellen, gruppiert nach Tag (Liniendiagramm) • Anzahl Spyware/Grayware-Ziele, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigste Spyware/Grayware (Balkendiagramm) • Allgemeine Zusammenfassung zu Spyware/Grayware (Rastertabelle) • Die 25 häufigsten Spyware/Grayware-Quellen (Balkendiagramm) • Zusammenfassung zu Spyware/Grayware-Quellen (Rastertabelle) • Die 25 häufigsten Spyware/Grayware-Ziele (Balkendiagramm) • Zusammenfassung zu Spyware/Grayware-Zielen (Rastertabelle) • Zusammenfassung zu Aktionsergebnissen (Kreisdiagramm) • Zusammenfassung zu Aktionen/Ergebnissen (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Lösung von verdächtigen Bedrohungen	Stellt die folgenden Informationen bereit: • Erkannte verdächtige Bedrohungen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Regelverstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Absender, gruppiert nach Tag (Liniendiagramm) • Anzahl der Empfänger, gruppiert nach Tag (Liniendiagramm) • Anzahl der Quellen-IP-Adressen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Ziel-IP-Adressen, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigsten Absender (Balkendiagramm) • Die 25 häufigsten Empfänger (Balkendiagramm) • Zusammenfassung zu Absendern verdächtiger Bedrohungen (Rastertabelle) • Zusammenfassung zu Empfängern der gefährlichsten verdächtigen Bedrohungen (Rastertabelle) • Die häufigsten 25 Quellen-IP-Adressen (Balkendiagramm) • Die häufigsten 25 Ziel-IP-Adressen (Balkendiagramm) • Zusammenfassung zu den Quellen verdächtiger Bedrohungen (Rastertabelle) • Zusammenfassung zu Zielen der gefährlichsten verdächtigen Bedrohungen (Rastertabelle) • Die 25 häufigsten Protokollnamen (Balkendiagramm) • Zusammenfassung zu Protokollzielen der verdächtigen Bedrohungen (Rastertabelle) • Allgemeine Zusammenfassung zu verdächtigen Bedrohungen (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Viren/Malware-Erkennung	Stellt die folgenden Informationen bereit: • Viren/Malware-Erkennung, gruppiert nach Tag (Liniendiagramm) • Anzahl eindeutiger Viren/Malware, gruppiert nach Tag (Liniendiagramm) • Anzahl der Infektionsziele, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigste Viren/Malware (Balkendiagramm) • Allgemeine Zusammenfassung zu Viren/Malware (Rastertabelle) • Die 25 häufigsten Infektionsquellen (Balkendiagramm) • Zusammenfassung zur Viren/Malware-Infektionsquellen (Rastertabelle) • Die 25 häufigsten Infektionsziele (Balkendiagramm) • Zusammenfassung zu Viren/Malware-Infektionszielen (Rastertabelle) • Zusammenfassung zu Aktionsergebnissen (Kreisdiagramm) • Zusammenfassung zu Viren/Malware (Rastertabelle)

VORLAGE	BESCHREIBUNG
TM - Zusammenfassung zur Erkennung von Verletzungen durch Internet-Bedrohungen	Stellt die folgenden Informationen bereit: • Erkennung von Verletzungen durch Internet-Bedrohungen, gruppiert nach Tag (Liniendiagramm) • Anzahl der Richtlinienverstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der Client-Verstöße, gruppiert nach Tag (Liniendiagramm) • Anzahl der URL-Verstöße, gruppiert nach Tag (Liniendiagramm) • Die 25 häufigsten Richtlinien mit Verstößen (Balkendiagramm) • Allgemeine Zusammenfassung zu Erkennung von Verletzungen durch Internet-Bedrohungen (Rastertabelle) • Die 25 häufigsten Clients mit Verstößen (Balkendiagramm) • Zusammenfassung zu Client-IP-Adressen bei Verletzungen durch Internet-Bedrohungen (Rastertabelle) • Die 25 häufigsten URLs mit Verstößen (Balkendiagramm) • Zusammenfassung zu URLs bei Verletzungen durch Internet-Bedrohungen (Rastertabelle) • Zusammenfassung Filter/Sperrtyp (Kreisdiagramm)

Grundlegendes zu Vorlagen für Control Manager 3

Control Manager enthält 87 im Vorfeld generierte Berichtvorlagen, die in sechs Kategorien unterteilt wurden: Kurzfassung, Gateway, Mail-Server, Server, Desktop, Netzwerkprodukte und Prävention vor Datenverlust.

Hinweis

In Control Manager 3.5 gelten Spyware und Grayware nicht mehr als Viren. Diese Änderung wirkt sich auf die Virenanzahl in allen ursprünglichen Virenberichten aus.

Die Berichterstellung kann, je nach Inhalt, einige Sekunden dauern. Sobald der Control Manager einen Bericht fertig gestellt hat, wird das Fenster aktualisiert, und der **View**-Link neben dem Bericht ist verfügbar.

Wählen Sie eine der unten aufgeführten sechs Berichtkategorien aus der Liste "Berichtkategorie" im Fenster "Control Manager" aus:

TABELLE A-15. Kurzfassungen und Berichtstypen

KURZFASSUNGEN	BERICHTTYPEN
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100) • Liste der gefundenen Spyware/ Grayware für alle Elemente
Berichte zu Virenfunden	• Virenfunde • Die am häufigsten gefundenen Viren (10, 25, 50, 100) • Liste der Vireninfektionen für alle Elemente
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat) • Säuberungsaufgaben, gruppiert nach (Tag, Woche, Monat) • Spam, gruppiert nach (Tag, Woche, Monat)

KURZFASSUNGEN	BERICHTTYPEN
Berichte zu Schwachstellen	• Bewertung der Risikostufe des PCs • Schwachstellenbewertung • Die am häufigsten gesäuberten Infektionen (10, 25, 50, 100) • Potenzielle Schwachstellen, die den größten Schaden anrichten (10, 25, 50, 100) • Schwachstellen nach Risikostufe

TABELLE A-16. Berichte und Berichtstypen für Gateway-Produkte

BERICHTE ZU GATEWAY-PRODUKTEN	BERICHTTYPEN
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100)
Berichte zu Virenfunden	• Virenfunde • Die am häufigsten gefundenen Viren (10, 25, 50, 100)
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Spam, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur Verteilungsrate	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zur Durchfallquote • OPS-Verteilungsrate für IMSS

TABELLE A-17. Berichte und Berichtstypen für Mail-Server-Produkte

BERICHTE ZU MAIL-SERVER-PRODUKTEN	BERICHTTYPEN
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100)
Berichte zu Virenfunden	• Virenfunde • Absender mit den meisten infizierten E-Mails (10, 25, 50, 100) • Die am häufigsten gefundenen Viren (10, 25, 50, 100)
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur Verteilungsrate	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zur Durchfallquote

TABELLE A-18. Berichte und Berichtstypen für serverbasierte Produkte

BERICHTE ZU SERVERBASIERTEN PRODUKTEN	BERICHTTYPEN
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Die am häufigsten gefundene Spyware/Grayware (10, 25, 50, 100)
Berichte zu Virenfunden	• Virenfunde • Die am häufigsten gefundenen Viren (10, 25, 50, 100)

Berichte zu serverbasierten Produkten	Berichttypen
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur Verteilungsrate	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zur Durchfallquote

Tabelle A-19. Berichte und Berichtstypen für Desktop-Produkte

Berichte zu Desktop-Produkten	Berichttypen
Berichte zu Spyware-/Grayware-Funden	• Spyware/Grayware erkannt • Am häufigsten erkannte Spyware/ Grayware (10, 25, 50,100)
Berichte zu Virenfunden	• Virenfunde • Am häufigsten erkannte Viren (10, 25, 50,100)
Berichte zu OfficeScan Client-Informationen	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung
Bericht zur OfficeScan Produktregistrierung	Registrierungsstatus
Vergleichende Berichte	• Spyware/Grayware, gruppiert nach (Tag, Woche, Monat) • Viren, gruppiert nach (Tag, Woche, Monat)
Berichte zur OfficeScan Server Verteilung	• Detaillierte Zusammenfassung • Grundlegende Zusammenfassung • Detaillierte Zusammenfassung zu Durchfallquoten

Berichte zu Desktop-Produkten	Berichttypen
Berichte zu Damage Cleanup Services von OfficeScan	• Detaillierte Zusammenfassung • Die am häufigsten gesäuberten Infektionen (10, 25, 50, 100)

Tabelle A-20. Berichte und Berichtstypen für Netzwerkprodukte

Berichte zu Netzwerkprodukten	Berichttypen
Berichte zu Network VirusWall	• Bericht zu Richtlinienverstößen, gruppiert nach (Tag, Woche, Monat) • Die am häufigsten gefundenen Clients mit Verstößen (10, 25, 50, 100) • Bericht zu Serviceverstößen, gruppiert nach (Tag, Woche, Monat)
Appliance-Berichte zu Trend Micro Total Discovery	• Zusammenfassung zu Vorfällen, gruppiert nach (Tag, Woche, Monat) • Clients mit hohem Risiko (10, 25, 50, 100) • Bericht mit Zusammenfassung bekannter und unbekannter Risiken

TABELLE A-21. Berichte und Berichtstypen zu Prävention vor Datenverlust

BERICHTE ZUR PRÄVENTION VOR DATENVERLUST	BERICHTTYPEN
Wichtigste Quellen für DLP-Vorfälle	• Vorfälle nach Absender (10, 20, 30, 40, 50) • Vorfälle nach Host-Name (10, 20, 30, 40, 50) • Vorfälle nach Empfänger (10, 20, 30, 40, 50) • Vorfälle nach Quellen-IP-Adresse (10, 20, 30, 40, 50) • Vorfälle nach URL (10, 20, 30, 40, 50) • Vorfälle nach Benutzer (10, 20, 30, 40, 50) • Wichtigste Vorlagenübereinstimmungen (10, 20, 30, 40, 50) • Verteilung der Vorfälle nach Kanal • Vorfalltrend, gruppiert nach (Tag, Woche, Monat) • Vorfälle nach Kanal, gruppiert nach (Tag, Woche, Monat)

Berichte zur Prävention vor Datenverlust	Berichttypen
Signifikanter Anstieg von Vorfällen	• Signifikanter Anstieg von Vorfällen (%) nach Kanal (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Kanal (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Absender (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Absender (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Host-Name (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Host-Name (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Benutzer (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Benutzer (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Quellen-IP-Adresse (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Quellen-IP-Adresse (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen (%) nach Vorlage (10, 20, 30, 40, 50) • Signifikanter Anstieg von Vorfällen nach Vorlage (10, 20, 30, 40, 50)

Einzelberichte hinzufügen

Sie können mit Control Manager Einzelberichte über die Berichtvorlagen Control Manager 3 und Control Manager 5 generieren. Benutzer müssen die Berichtvorlagen vom Typ Control Manager 5 erstellen, während Trend Micro die Berichtvorlagen vom

Typ Control Manager 3 erstellt hat. Die Arbeitsschritte zum Erstellen eines Einzelberichts ähneln sich für alle Berichtstypen und umfassen Folgendes:

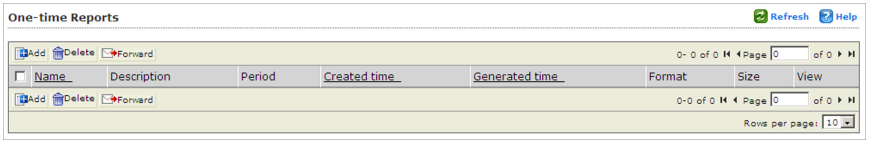
1. Öffnen Sie das Fenster **Add One-time Report**, und wählen Sie den Berichttyp.
2. Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden:
3. Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.
4. Geben Sie den Empfänger des Berichts an.

Schritt 1: Öffnen Sie das Fenster "Einzelbericht hinzufügen", und wählen Sie den Berichttyp.

Prozedur

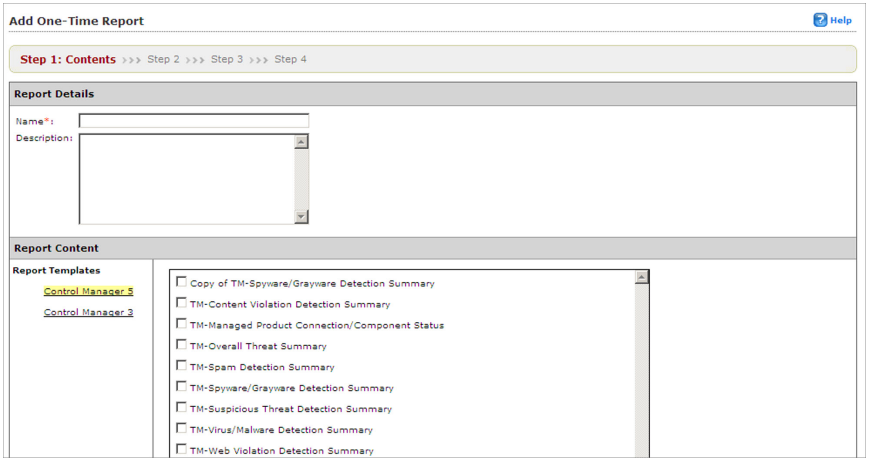
1. Navigieren Sie zu **Reports** > **One-time Reports**.

   Das Fenster **One-time Reports** wird angezeigt.



2. Klicken Sie auf **Add**.

   Das Fenster **Add One-time Report > Step 1: Contents** wird angezeigt.



3. Geben Sie einen Namen für den Bericht unter "Berichtdetails" in das Feld **Name** ein.

4. Geben Sie eine Beschreibung für den Bericht unter "Berichtdetails" in das Feld **Description** ein.

5. Wählen Sie die Control Manager Vorlage, anhand der der Bericht generiert werden soll:

   - **Berichtvorlage Control Manager 5**:

     a. Wählen Sie die Control Manager 5 Vorlage, anhand der der Bericht generiert werden soll: Wenn die vorhandenen Berichte Ihre Anforderungen nicht erfüllen, erstellen Sie eine neue Vorlage über das Fenster **Report Templates**.

   - **Berichtvorlage Control Manager 3**:

     a. Klicken Sie unter Berichtinhalt auf **Control Manager 3**. Die Control Manager 3 Vorlagen werden im Arbeitsbereich auf der rechten Seite unter "Berichtinhalt" angezeigt.

     b. Wählen Sie die Berichtkategorie, die als Grundlage für den Bericht dient.

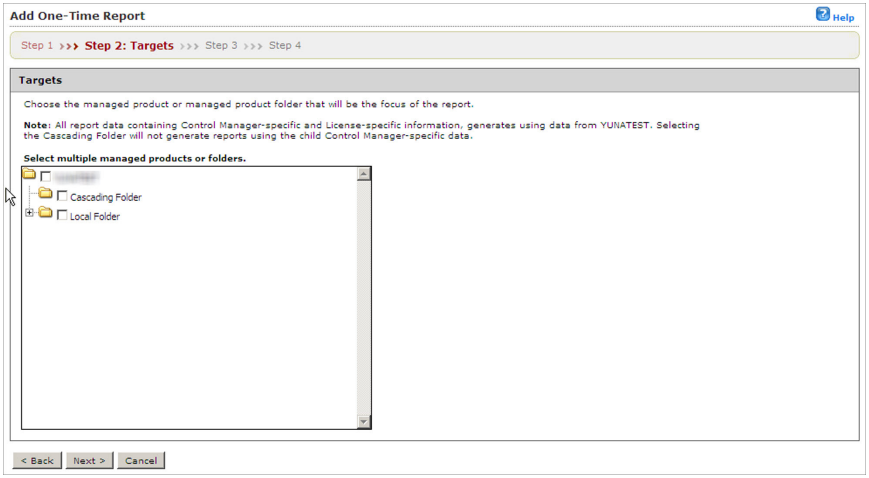
     c. Wählen Sie die Control Manager 3 Vorlagendaten, auf denen die Vorlage basiert.

6. Wählen Sie das Format für den generierten Bericht:

   - **Berichtformate für Control Manager 5**:
     - Adobe PDF Format (*.pdf)
     - HTML-Format (*.html)
     - XML-Format (*.xml)
     - CSV-Format (*.csv)
   - **Berichtformate für Control Manager 3**:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)

7. Klicken Sie auf **Next**.

   Das Fenster **Add One-Time Report > Step 2: Targets** wird angezeigt.

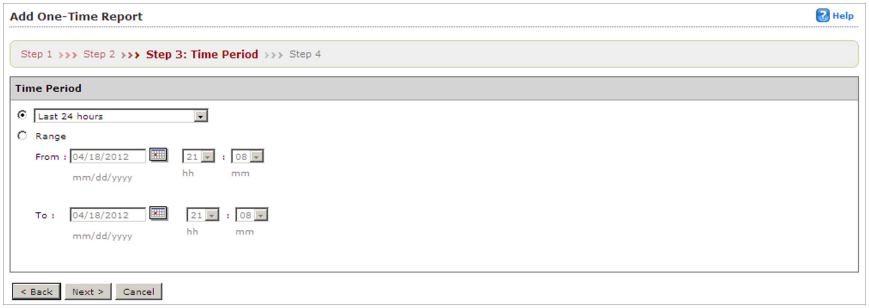

Add One-Time Report
Help
Step 1 >>> Step 2: Targets >>> Step 3 >>> Step 4
Targets
Choose the managed product or managed product folder that will be the focus of the report.
Note: All report data containing Control Manager-specific and License-specific information, generates using data from YUNATEST. Selecting the Cascading Folder will not generate reports using the child Control Manager-specific data.
Select multiple managed products or folders.
Cascading Folder
Local Folder
< Back
Next >
Cancel

Schritt 2: Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden:

Prozedur

1. Wählen Sie das verwaltete Produkt oder Verzeichnis, aus dem Control Manager die Berichtinformationen erfasst.
2. Wenn der Bericht Daten von einem Network VirusWall Enforcer Gerät enthält, geben Sie die Clients für die Berichtgenerierung an:
   - **All clients**: Berichte werden von allen Network VirusWall Enforcer Geräten generiert
   - **IP range**: Berichte werden auf Grundlage eines bestimmten IP-Adressbereichs generiert
   - **Segment**: Berichte werden auf Grundlage eines bestimmten Netzwerksegments generiert
3. Klicken Sie auf **Next**.

   Das Fenster **Add One-Time Report > Step 3: Time Period** wird angezeigt.



Schritt 3: Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.

Prozedur

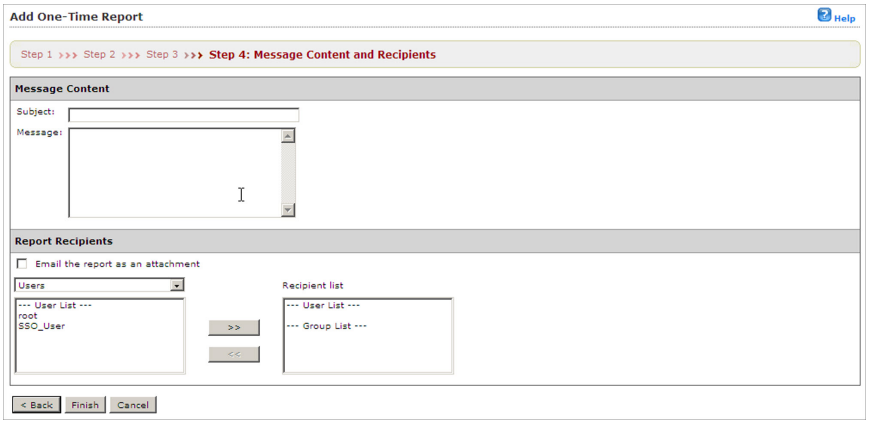
1. Geben Sie das Datum an, an dem die Daten generiert werden sollen:
   - Wählen Sie aus dem Listenfeld eine der folgenden Optionen aus:
     - Gesamter Zeitraum
     - Letzte 24 Stunden
     - Heute
     - Letzte 7 Tage
     - Letzte 14 Tage
     - Letzte 30 Tage
   - Geben Sie einen Datumsbereich an:
     - Geben Sie ein Datum in das Feld **From** ein.
     - Geben Sie eine Uhrzeit in die betreffenden Felder **hh** und **mm** ein.
     - Geben Sie ein Datum in das Feld **To** ein.
     - Geben Sie eine Uhrzeit in die betreffenden Felder **hh** und **mm** ein.

   Hinweis

   Klicken Sie auf das Kalendersymbol neben den Feldern **From** und **To**, um den Datumsbereich über den dynamischen Kalender festzulegen.

2. Klicken Sie auf **Next**.

   Das Fenster **Add Onetime Report > Step 4: Message Content and Recipients screen** wird angezeigt.



Schritt 4: Geben Sie den Empfänger des Berichts an:

Prozedur

1. Geben Sie eine Betreffzeile für die E-Mail-Nachricht mit dem Bericht in das Feld **Subject** ein.
2. Geben Sie eine Beschreibung des Berichts in das Feld **Message** ein.
3. Wählen Sie **Email the report as an attachment**, um den Bericht an den angegebenen Empfänger zu versenden.
4. Aktivieren Sie diese Option, um Benutzer oder Gruppen aus der Liste **Report Recipients** auszuwählen.
5. Wählen Sie die Benutzer/Gruppen, die den Bericht erhalten sollen, und klicken Sie auf die Schaltfläche **>>**.
6. Klicken Sie auf **Finish**, nachdem Sie alle Benutzer/Gruppen ausgewählt haben, die den Bericht erhalten sollen.

Zeitgesteuerte Berichte hinzufügen

Sie können mit Control Manager zeitgesteuerte Berichte über die Berichtvorlagen Control Manager 3 und Control Manager 5 generieren. Benutzer müssen die Berichtvorlagen vom Typ Control Manager 5 erstellen, während Trend Micro die Berichtvorlagen vom Typ Control Manager 3 erstellt hat. Die Schritte zum Erstellen eines zeitgesteuerten Berichts ähneln sich für alle Berichtstypen:

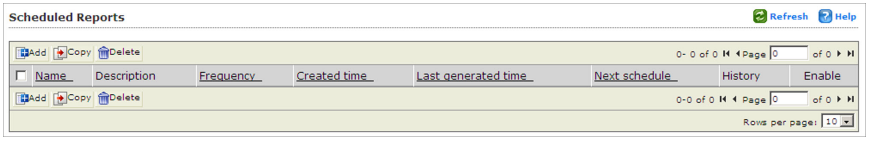
1. Öffnen Sie das Fenster **Add Scheduled Report**, und wählen Sie den Berichttyp.
2. Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden:
3. Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.
4. Geben Sie den Empfänger des Berichts an.

Schritt 1: Öffnen Sie das Fenster "Zeitgesteuerten Bericht hinzufügen", und wählen Sie den Berichttyp.

Prozedur

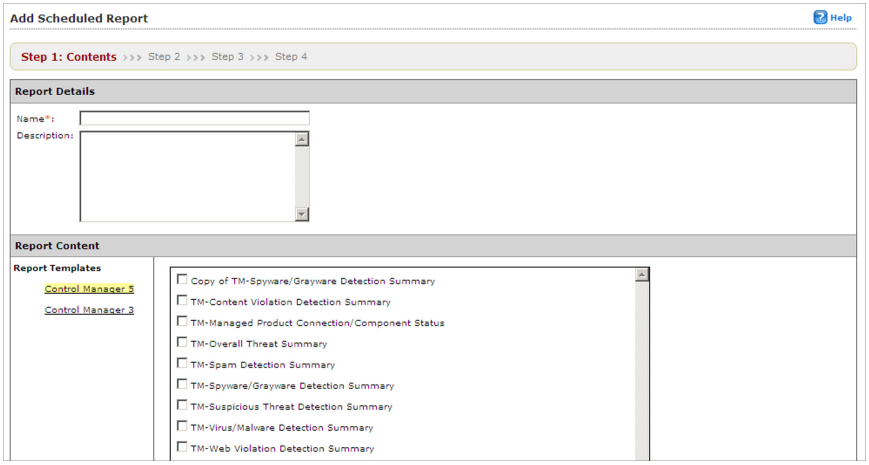
1. Navigieren Sie zu **Reports** > **Scheduled Reports**.

   Das Fenster **Scheduled Reports** wird angezeigt.



2. Klicken Sie auf **Add**.

   Das Fenster **Add Scheduled Report > Step 1: Contents** wird angezeigt.



3. Geben Sie einen Namen für den Bericht in das Feld **Name** ein.

4. Geben Sie eine aussagekräftige Beschreibung für den Bericht in das Feld **Description** ein.

5. Wählen Sie die Control Manager Vorlage, anhand der der Bericht generiert werden soll:

   - Berichtvorlage Control Manager 5:

     a. Wählen Sie die Control Manager 5 Vorlage, anhand der der Bericht generiert werden soll: Wenn die vorhandenen Berichte Ihre Anforderungen nicht erfüllen, erstellen Sie eine neue Vorlage über das Fenster "Berichtvorlagen".

   - Berichtvorlage Control Manager 3:

     a. Klicken Sie unter Berichtinhalt auf **Control Manager 3**. Die Control Manager 3 Vorlagen werden im Arbeitsbereich auf der rechten Seite unter "Berichtinhalt" angezeigt.

     b. Wählen Sie die Berichtkategorie, die als Grundlage für den Bericht dient.

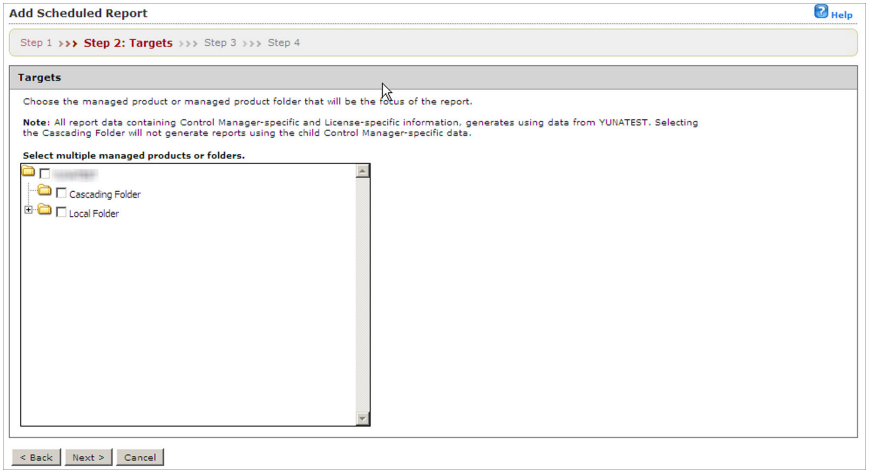
     c. Wählen Sie die Control Manager 3 Vorlagendaten, auf denen die Vorlage basiert.

6. Wählen Sie das Format für den generierten Bericht:

   - Berichtformate für Control Manager 5:
     - Adobe PDF Format (*.pdf)
     - HTML-Format (*.html)
     - XML-Format (*.xml)
     - CSV-Format (*.csv)
   - Berichtformate für Control Manager 3:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)

7. Klicken Sie auf **Next**.

   Das Fenster **Add Scheduled Report > Step 2: Targets** wird angezeigt.


Add Scheduled Report
Help
Step 1 >>> Step 2: Targets >>> Step 3 >>> Step 4
Targets
Choose the managed product or managed product folder that will be the focus of the report.
Note: All report data containing Control Manager-specific and License-specific information, generates using data from YUNATEST. Selecting the Cascading Folder will not generate reports using the child Control Manager-specific data.
Select multiple managed products or folders.
Cascading Folder
Local Folder
< Back
Next >
Cancel

Schritt 2: Geben Sie das bzw. die Produkte an, aus denen die Berichtsdaten generiert werden.

Prozedur

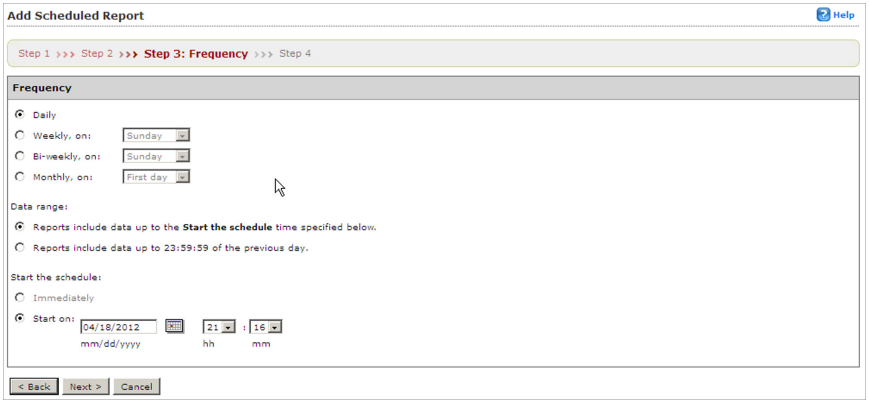
1. Wählen Sie das verwaltete Produkt oder Verzeichnis, aus dem Control Manager die Berichtinformationen erfasst.

2. Wenn der Bericht Daten von einem Network VirusWall Enforcer Gerät enthält, geben Sie die Clients für die Berichtgenerierung an:

   - **All clients**: Berichte werden von allen Network VirusWall Enforcer Geräten generiert
   - **IP range**: Berichte werden auf Grundlage eines bestimmten IP-Adressbereichs generiert
   - **Segment**: Berichte werden auf Grundlage eines bestimmten Netzwerksegments generiert

3. Klicken Sie auf **Next**.

   Das Fenster **Add One-Time Report > Step 3: Frequency** wird angezeigt.



Schritt 3: Geben Sie das Datum an, an dem das bzw. die Produkte die Daten erzeugen soll.

Prozedur

1. Geben Sie an, wie oft die Berichte generiert werden sollen:
   - **Daily**: Berichte werden täglich generiert.
   - **Weekly**: Berichte werden wöchentlich am angegebenen Tag generiert.
   - **Bi-weekly**: Berichte werden alle zwei Wochen am angegebenen Tag generiert.
   - **Monthly**: Berichte werden monatlich am ersten Tag des Monats, am 15. des Monats oder am letzten Tag des Monats generiert.
2. Geben Sie einen Datumsbereich an:
   - **Reports include data up to the Start the schedule time specified below**: Das bedeutet, ein Bericht kann bis zu 23 Stunden mehr Daten enthalten. Während sich dies nur unwesentlich auf die wöchentlichen oder monatlichen Berichte auswirkt, können "tägliche" Berichte abhängig vom Beginn der Planungszeit die Daten von fast zwei Tagen enthalten.
   - **Reports include data up to 23:59:59 of the previous day**: Das bedeutet, dass die Datenerfassung für den Bericht erst kurz vor Mitternacht beendet wird. Berichte mit einer genauen Zeitperiode (Beispiel: Tägliche Berichte enthalten 24 Stunden), jedoch ohne die absolut letzten Daten.
3. Geben Sie an, wann der Berichtzeitplan beginnen soll:
   - **Immediately**: Der Berichtzeitplan beginnt sofort nachdem der Bericht aktiviert wurde.
   - **Start on**: Der Berichtzeitplan beginnt am Datum und an der Uhrzeit, die in den betreffenden Feldern festgelegt ist.

   a. Geben Sie ein Datum in das Feld **mm/dd/yyyy** ein.

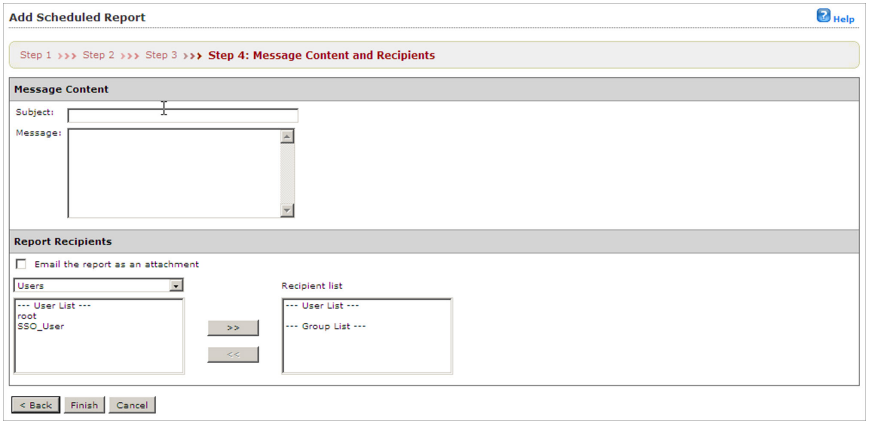
   b. Geben Sie eine Uhrzeit in die betreffenden Felder **hh** und **mm** ein.

Hinweis

Klicken Sie auf das Kalendersymbol neben dem Feld **mm/dd/yyyy**, um den Datumsbereich über den dynamischen Kalender festzulegen.

4. Klicken Sie auf **Next**.

   Das Fenster **Add Scheduled Report > Step 4: Message Content and Recipients** wird angezeigt.



Schritt 4: Geben Sie den Empfänger des Berichts an

Prozedur

1. Geben Sie eine Betreffzeile für die E-Mail-Nachricht mit dem Bericht in das Feld **Subject** ein.
2. Geben Sie eine Beschreibung des Berichts in das Feld **Message** ein.
3. Wählen Sie **Email the report as an attachment**, um den Bericht an den angegebenen Empfänger zu versenden.
4. Aktivieren Sie diese Option, um Benutzer oder Gruppen aus der Liste **Report Recipients** auszuwählen.

5. Wählen Sie die Benutzer/Gruppen, die den Bericht erhalten sollen, und klicken Sie auf die Schaltfläche **>>**.

6. Klicken Sie auf **Finish**, nachdem Sie alle Benutzer/Gruppen ausgewählt haben, die den Bericht erhalten sollen.

Anhang B

PolicyServer Nachrichten-IDs

In der folgenden Tabelle werden die Fehlermeldungen von PolicyServer beschrieben. Ermitteln Sie anhand dieser Angaben die Nachrichten-ID, um die Bedeutung der zugehörigen Meldung, die Kategorie der Meldung und auf welche Agents/Produkte sich die Meldung auswirkt, zu verstehen.

TABELLE B-1. POLICYSERVER NACHRICHTEN-IDS

KATEGORIE	NACHRICHTEN -ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	100002	Gerät wird identifiziert	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100003	Sicherheitsverstoß	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100007	Kritischer Schweregrad	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	100019	Ändern der Richtlinie fehlgeschlagen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100045	Nicht unterstützte Konfiguration	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100046	Unternehmenspool erstellt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100047	Unternehmenspool gelöscht	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100048	Unternehmenspool geändert	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100049	Admin-Benutzer auf Grund zu vieler fehlgeschlagener Anmeldungen gesperrt.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100052	Integritätsprüfung des Richtlinienwerts fehlgeschlagen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	100053	Richtlinienanforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100054	Dateianforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100055	Admin-Authentifizierung erfolgreich	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100056	Admin-Authentifizierung fehlgeschlagen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100062	Admin-Kennwort zurückgesetzt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100463	Benutzer kann nicht entfernt werden. Versuchen Sie es erneut.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	100464	Benutzer kann nicht deaktiviert werden. Versuchen Sie es erneut.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100470	Selbsthilfe-Kennwort kann nicht geändert werden. Eine Antwort auf eine der persönlichen Herausforderungsfragen war falsch.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	102000	Unternehmen hinzugefügt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	102001	Unternehmen gelöscht	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	102002	Unternehmen geändert	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	102003	Die Anzahl der Benutzer hat das unter dieser Lizenz zulässige Maximum überschritten. Verringern Sie die Anzahl der vorhandenen Benutzer, um dieses Benutzerkonto wiederherzustellen.	PolicyServer
Administratorwarnungen	200000	Administrator hat Richtlinie aktualisiert	PolicyServer
Administratorwarnungen	200001	Administrator hat Richtlinie hinzugefügt	PolicyServer
Administratorwarnungen	200002	Administrator hat Richtlinie gelöscht	PolicyServer
Administratorwarnungen	200003	Administrator hat Richtlinie aktiviert	PolicyServer
Administratorwarnungen	200004	Administrator hat Richtlinie deaktiviert	PolicyServer
Administratorwarnungen	200100	Administrator hat Benutzer hinzugefügt	PolicyServer
Administratorwarnungen	200101	Administrator hat Benutzer gelöscht	PolicyServer
Administratorwarnungen	200102	Administrator hat Benutzer aktualisiert	PolicyServer
Administratorwarnungen	200103	Administrator hat Benutzer zu Gruppe hinzugefügt	PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	200104	Administrator hat Benutzer von Gruppe entfernt	PolicyServer
Administratorwarnungen	200200	Benutzer hinzugefügt	PolicyServer
Administratorwarnungen	200201	Benutzer gelöscht	PolicyServer
Administratorwarnungen	200202	Benutzer zu Gruppe hinzugefügt	PolicyServer
Administratorwarnungen	200203	Benutzer von Gruppe entfernt	PolicyServer
Administratorwarnungen	200204	Benutzer aktualisiert	PolicyServer
Administratorwarnungen	200300	Administrator hat Gerät gelöscht	PolicyServer
Administratorwarnungen	200301	Administrator hat Gerät zu Gruppe hinzugefügt	PolicyServer
Administratorwarnungen	200302	Administrator hat Gerät von Gruppe entfernt	PolicyServer
Administratorwarnungen	200500	Administrator hat Gruppe hinzugefügt	PolicyServer
Administratorwarnungen	200501	Administrator hat Gruppe gelöscht	PolicyServer
Administratorwarnungen	200502	Administrator hat Gruppe aktualisiert	PolicyServer
Administratorwarnungen	200503	Administrator hat Gruppe kopiert/ eingefügt	PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	200600	Update des PolicyServer angewendet.	PolicyServer
Administratorwarnungen	200602	Benutzer zu Gerät hinzugefügt	PolicyServer
Administratorwarnungen	200603	Benutzer von Gerät entfernt	PolicyServer
Administratorwarnungen	200700	Ereignis ausgeführt	PolicyServer
Administratorwarnungen	200701	Ereignisausführung fehlgeschlagen	PolicyServer
Administratorwarnungen	200800	Ereignis installiert	PolicyServer
Administratorwarnungen	200801	Installation des Ereignisses fehlgeschlagen	PolicyServer
Administratorwarnungen	700012	Angemeldeter Administrator verwendet Einmalkennwort	File Encryption SP6 oder früher
Administratorwarnungen	700013	Angemeldeter Administrator verwendet festes Kennwort	File Encryption SP6 oder früher
Administratorwarnungen	700014	Angemeldeter Administrator verwendet Smartcard	File Encryption SP6 oder früher
Administratorwarnungen	700017	Angemeldeter Administrator verwendet Remote-Authentifizierung	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	700030	Anmelden des Administrators mit Einmalkennwort ist fehlgeschlagen	File Encryption SP6 oder früher
Administratorwarnungen	700031	Anmelden des Administrators mit festem Kennwort ist fehlgeschlagen	File Encryption SP6 oder früher
Administratorwarnungen	700032	Anmelden des Administrators mit Smartcard ist fehlgeschlagen	File Encryption SP6 oder früher
Administratorwarnungen	700035	Anmelden des Administrators mit der Remote-Authentifizierung ist fehlgeschlagen	File Encryption SP6 oder früher
Administratorwarnungen	900100	Angemeldeter Administrator verwendet Einmalkennwort.	KeyArmor
Administratorwarnungen	900101	Angemeldeter Administrator verwendet festes Kennwort.	KeyArmor
Administratorwarnungen	900102	Angemeldeter Administrator verwendet Smartcard.	KeyArmor
Administratorwarnungen	900103	Angemeldeter Administrator verwendet Domänenauthentifizierung.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	900104	Angemeldeter Administrator verwendet Remote-Authentifizierung.	KeyArmor
Administratorwarnungen	900105	Angemeldeter Administrator verwendet ColorCode-Authentifizierung.	KeyArmor
Administratorwarnungen	900106	Angemeldeter Administrator verwendet PIN.	KeyArmor
Administratorwarnungen	900107	Angemeldeter Administrator verwendet OCSP.	KeyArmor
Administratorwarnungen	900250	Anmelden des Administrators mit Einmalkennwort ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900251	Anmelden des Administrators mit festem Kennwort ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900252	Anmelden des Administrators mit Smartcard ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900253	Anmelden des Administrators mit Domänenauthentifizierung ist fehlgeschlagen.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Administratorwarnungen	900254	Anmelden des Administrators mit Remote-Authentifizierung ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900255	Anmelden des Administrators mit ColorCode-Authentifizierung ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900256	Anmelden des Administrators mit PIN ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900257	Anmelden des Administrators mit OCSP ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900300	Anmelden des Administrators mit der Remote-Authentifizierung ist fehlgeschlagen	KeyArmor
Administratorwarnungen	901000	Administrator hat eine Datei umbenannt	KeyArmor
Administratorwarnungen	901001	Administrator hat eine Datei geändert	KeyArmor
Administratorwarnungen	901002	Administrator hat eine Datei gelöscht	KeyArmor
Administratorwarnungen	901003	Administrator hat eine Datei erstellt	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Audit-Protokoll-Warnungen	100015	Protokollmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103000	Audit-Protokoll-Verbindung geöffnet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103001	Audit-Protokoll-Verbindung geschlossen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103100	Audit-Protokoll-Datensatz fehlt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103101	Keine Integrität bei Audit-Protokoll-Datensatz	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103102	Integrität von Audit-Protokoll-Datensatz gefährdet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103103	Validierung der Integrität des Audit-Protokoll-Datensatzes gestartet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Audit-Protokoll-Warnungen	104003	Authentifizierungsmethode auf Smartcard festgelegt.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	904008	Protokollwarnung kann nicht gesendet werden	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Authentifiziererwarnungen	700006	Angemeldeter Authentifizierer verwendet Einmalkennwort	File Encryption SP6 oder früher
Authentifiziererwarnungen	700007	Angemeldeter Authentifizierer verwendet festes Kennwort	File Encryption SP6 oder früher
Authentifiziererwarnungen	700008	Angemeldeter Authentifizierer verwendet Smartcard	File Encryption SP6 oder früher
Authentifiziererwarnungen	700009	Angemeldeter Authentifizierer verwendet Windows Anmeldedaten	File Encryption SP6 oder früher
Authentifiziererwarnungen	700011	Angemeldeter Authentifizierer verwendet Remote-Authentifizierung	File Encryption SP6 oder früher
Authentifiziererwarnungen	700024	Anmelden des Authentifizierers mit Einmalkennwort ist fehlgeschlagen	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Authentifiziererwarnungen	700025	Anmelden des Authentifizierers mit festem Kennwort ist fehlgeschlagen	File Encryption SP6 oder früher
Authentifiziererwarnungen	700026	Anmelden des Authentifizierers mit Smartcard ist fehlgeschlagen	File Encryption SP6 oder früher
Authentifiziererwarnungen	700027	Anmelden des Authentifizierers mit Windows Anmeldedaten ist fehlgeschlagen	File Encryption SP6 oder früher
Authentifiziererwarnungen	700029	Anmelden des Authentifizierers mit der Remote-Authentifizierung ist fehlgeschlagen	File Encryption SP6 oder früher
Authentifiziererwarnungen	900050	Angemeldeter Authentifizierer verwendet Einmalkennwort.	KeyArmor
Authentifiziererwarnungen	900051	Angemeldeter Authentifizierer verwendet festes Kennwort.	KeyArmor
Authentifiziererwarnungen	900052	Angemeldeter Authentifizierer verwendet Smartcard.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Authentifiziererwarnungen	900053	Angemeldeter Authentifizierer verwendet Domänenauthentifizierung.	KeyArmor
Authentifiziererwarnungen	900054	Angemeldeter Authentifizierer verwendet Remote-Authentifizierung.	KeyArmor
Authentifiziererwarnungen	900055	Angemeldeter Authentifizierer verwendet ColorCode-Authentifizierung.	KeyArmor
Authentifiziererwarnungen	900056	Angemeldeter Authentifizierer verwendet PIN.	KeyArmor
Authentifiziererwarnungen	900057	Angemeldeter Authentifizierer verwendet OCSP.	KeyArmor
Authentifiziererwarnungen	900161	Anmelden des Benutzers mit Selbsthilfe ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900200	Anmelden des Authentifizierers mit Einmalkennwort ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900201	Anmelden des Authentifizierers mit festem Kennwort ist fehlgeschlagen.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Authentifiziererwarnungen	900202	Anmelden des Authentifizierers mit Smartcard ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900203	Anmelden des Authentifizierers mit Domänenauthentifizierung ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900204	Anmelden des Authentifizierers mit Remote-Authentifizierung ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900205	Anmelden des Authentifizierers mit ColorCode-Authentifizierung ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900206	Anmelden des Authentifizierers mit PIN ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900207	Anmelden des Authentifizierers mit OCSP ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	902000	Authentifizierer hat eine Datei umbenannt	KeyArmor
Authentifiziererwarnungen	902001	Authentifizierer hat eine Datei geändert	KeyArmor
Authentifiziererwarnungen	902002	Authentifizierer hat eine Datei gelöscht	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Authentifiziererwarnungen	902003	Authentifizierer hat eine Datei erstellt	KeyArmor
Zertifikatswarnungen	104008	Zertifikat abgelaufen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100001	Authentifizierung für die Synchronisierung zwischen PDA und Desktop war nicht erfolgreich. Es wurde für diesen PDA keine Geräte-ID gefunden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100012	Gerät befindet sich nicht in seiner eigenen Kennwortauthentifizierungsdatei. PAF beschädigt?	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100044	Aktion zum Sperren von Geräten empfangen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100071	Auslöschen des Geräts bestätigt	KeyArmor
Gerätewarnungen	100072	Gerätesperre bestätigt	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Gerätewarnungen	100100	Installation gestartet	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor
Gerätewarnungen	100101	Installation abgeschlossen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor
Gerätewarnungen	100462	Verbindung mit PolicyServer nicht möglich.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	101001	Die Netzwerkverbindung funktioniert nicht. Die Richtliniendateien können nicht vom PolicyServer abgerufen werden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	101002	Beschädigte PAF-Datei (DAFolder.xml)	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	105000	Richtlinien können nicht mit Client synchronisiert werden. Überprüfen Sie, ob eine Netzwerkverbindung vorhanden ist, und versuchen Sie es erneut.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Gerätewarnungen	200400	Gerät hinzugefügt	PolicyServer
Gerätewarnungen	200401	Gerät gelöscht	PolicyServer
Gerätewarnungen	200402	Gerät zu Gruppe hinzugefügt	PolicyServer
Gerätewarnungen	200403	Gerät von Gruppe entfernt	PolicyServer
Gerätewarnungen	200404	Gerät geändert	PolicyServer
Gerätewarnungen	200405	Gerätestatus aktualisiert	PolicyServer
Gerätewarnungen	200406	Gerätestatus zurückgesetzt	PolicyServer
Gerätewarnungen	200407	Auslöschen des Geräts ausgelöst	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	200408	Gerätesperre ausgestellt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	200409	Gerät synchronisiert	PolicyServer
Gerätewarnungen	904012	Der Benutzer darf kein neues Gerät registrieren.	PolicyServer
Gerätewarnungen	1000052	Deinstallation des Produkts	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Gerätewarnungen	1000053	Deinstallation des Produkts von Richtlinie verweigert	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor
Fehlerwarnungen	100005	Allgemeiner Fehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Fehlerwarnungen	100006	Anwendungsfehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Warnungen bei File Encryption Aktivität	700000	Angemeldeter Benutzer verwendet Einmalkennwort	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700001	Angemeldeter Benutzer verwendet festes Kennwort	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700002	Angemeldeter Benutzer verwendet Smartcard	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700003	Angemeldeter Benutzer verwendet Windows Anmeldedaten	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700005	Angemeldeter Benutzer verwendet Remote-Authentifizierung	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei File Encryption Aktivität	700015	Angemeldeter Administrator verwendet Windows Anmeldedaten	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700018	Anmelden des Benutzers mit Einmalkennwort ist fehlgeschlagen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700019	Anmelden des Benutzers mit festem Kennwort ist fehlgeschlagen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700020	Anmelden des Benutzers mit Smartcard ist fehlgeschlagen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700021	Anmelden des Benutzers mit Windows Anmeldedaten ist fehlgeschlagen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700023	Benutzer konnte sich mit der Remote-Authentifizierung nicht anmelden	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	700033	Anmelden des Administrators mit Windows Anmeldedaten ist fehlgeschlagen	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei File Encryption Aktivität	700036	Anzahl fehlgeschlagener Anmeldeversuche überschritten	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701000	Verschlüsselte Datei unter Verwendung eines Benutzerschlüssels	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701001	Verschlüsselte Datei unter Verwendung eines Gruppenschlüssels	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701002	Verschlüsselte Datei unter Verwendung eines statischen Kennworts	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701003	Selbstextrahierende, verschlüsselte Datei, die unter Verwendung eines statischen Kennworts erstellt wurde.	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701004	Verschlüsselte Datei unter Verwendung eines Zertifikats	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701005	Selbstextrahierende, verschlüsselte Datei, die unter Verwendung eines Zertifikats erstellt wurde.	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei File Encryption Aktivität	701006	Verschlüsselte Datei unter Verwendung eines CD/DVD-Brennvorgangs	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701007	Verschlüsseltes Verzeichnis unter Verwendung eines Gruppenschlüssels	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701008	Verschlüsseltes Verzeichnis unter Verwendung eines statischen Kennworts	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701009	Selbstextrahierendes, verschlüsseltes Verzeichnis, das unter Verwendung eines statischen Kennworts erstellt wurde.	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701010	Verschlüsseltes Verzeichnis unter Verwendung eines Zertifikats	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701011	Selbstextrahierendes, verschlüsseltes Verzeichnis, das unter Verwendung eines Zertifikats erstellt wurde.	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701012	Verschlüsselter Ordner unter Verwendung eines CD/DVD-Brennvorgangs	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei File Encryption Aktivität	701015	Wechselmedium wurde vollständig verschlüsselt	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701016	Wechselmedium gesperrt	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701017	Auf Wechselmedium wurden Ordner erstellt und einbezogen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701018	Datei verschlüsselt und auf Wechselmedium verschoben.	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	701019	Datei von Wechselmedium gelöscht.	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703000	Mit FileArmor verschlüsselter Ordner wurde erstellt	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703001	Ordner wurde erstellt und einbezogen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703002	Mit FileArmor verschlüsselter Ordner wurde gelöscht	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703004	Auf Wechselmedium wurde Ordner erstellt und einbezogen	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei File Encryption Aktivität	703005	Wechseldatenträger wurde vollständig verschlüsselt	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703006	Datei in Ordner wurde erstellt	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703007	Datei in Ordner wurde gelöscht	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703008	Datei in Ordner wurde geändert	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703009	Auf Datei in Ordner wurde zugegriffen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703010	Datei in Ordner wurde zuletzt geschrieben	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703011	Dateigröße in Ordner geändert	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703015	Ordnerverschlüsselung gestartet	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703016	Ordnerentschlüsselung gestartet	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703017	Ordnerverschlüsselung abgeschlossen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703018	Ordnerentschlüsselung abgeschlossen	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703019	Ordnerentschlüsselung läuft	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	703020	Ordnerverschlüsselung läuft	File Encryption SP6 oder früher

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei File Encryption Aktivität	704000	File Encryption Dienst wurde gestartet	File Encryption SP6 oder früher
Warnungen bei File Encryption Aktivität	704001	File Encryption Dienst wurde heruntergefahren	File Encryption SP6 oder früher
Warnungen bei Full Disk Encryption	300700	Maximale Größe des Geräteprotokolls erreicht, Ereignisprotokoll wird abgeschnitten.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400001	Benutzer hat sich angemeldet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400002	Benutzeranmeldung fehlgeschlagen.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400003	Geräteentschlüsselung gestartet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400004	Geräteverschlüsselung gestartet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400005	Verschlüsselte Partition gemountet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400006	Nativer OS-MBR wiederhergestellt.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400007	Anwendungs-MBR wiederhergestellt.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400008	Geräteverschlüsselung abgeschlossen	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400009	Geräteentschlüsselung abgeschlossen	Full Disk Encryption oder MobileSentinel

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	400010	Geräteverschlüsselung wird durchgeführt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400011	System-MBR beschädigt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400012	Preboot-Kernel des Systems gelöscht	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401000	Zugriff auf Wiederherstellungskonsole	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401009	Fehler bei Wiederherstellungskonsole	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401010	In-Place-Entschlüsselung gestartet	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401011	In-Place-Entschlüsselung gestoppt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401012	In-Place-Entschlüsselung abgeschlossen	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401013	Entschlüsselung des Wechseldatenträgers gestartet	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401014	Entschlüsselung des Wechseldatenträgers gestoppt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401015	Entschlüsselung des Wechseldatenträgers abgeschlossen	Full Disk Encryption oder MobileSentinel

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	401018	Fehler bei In-Place-Entschlüsselung	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401019	Fehler bei Entschlüsselung des Wechseldatenträgers	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401020	Zugriff auf verschlüsselte Dateien	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401021	Verschlüsselte Dateien geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401022	Verschlüsselte Dateien auf Wechseldatenträger kopiert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401029	Fehler beim Zugriff auf verschlüsselte Dateien	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401030	Zugriff auf Netzwerkadministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401031	PolicyServer Adresse geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401032	PolicyServer Portnummer geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401033	Zu IPv6 gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401034	Zu IPv4 gewechselt	Full Disk Encryption oder MobileSentinel

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	401035	Zur dynamischen IP-Konfiguration gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401036	Zur statischen IP-Konfiguration gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401037	DHCP-Portnummer geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401038	IP-Adresse geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401039	Netzmaske geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401040	Broadcast-Adresse geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401041	Gateway geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401042	Domänenname geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401043	Domain Name Server geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401049	Fehler bei Netzwerkadministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401050	Zugriff auf Benutzeradministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401051	Benutzer hinzugefügt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401052	Benutzer entfernt	Full Disk Encryption oder MobileSentinel

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	401053	Benutzer geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401069	Fehler bei Benutzeradministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401070	Zugriff auf lokal gespeicherte Protokolle	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401079	Fehler bei Zugriff auf lokal gespeicherte Protokolle	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401080	Ursprünglicher MBR wiederhergestellt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401089	Fehler beim Wiederherstellen des ursprünglichen MBR	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401090	Standarddesign wiederhergestellt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401099	Fehler bei Wiederherstellung des Standarddesigns	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	402000	Start der Anwendung	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	402001	Herunterfahren der Anwendung	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	600001	Preboot-Update war erfolgreich.	Full Disk Encryption

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	600002	Preboot-Update fehlgeschlagen	Full Disk Encryption
Installationswarnungen	100004	Installationsfehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Installationswarnungen	100020	Erfolgreiche Installation	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Installationswarnungen	700037	Die Installation der File Encryption war erfolgreich.	File Encryption SP6 oder früher
Installationswarnungen	700038	Die Installation der File Encryption war nicht erfolgreich. Unternehmensname ist nicht gültig.	File Encryption SP6 oder früher
Installationswarnungen	700039	Die Installation der File Encryption war nicht erfolgreich. Benutzername oder Kennwort ist falsch.	File Encryption SP6 oder früher
Warnungen bei KeyArmor Aktivität	100034	Ungültige Registrierungseinstellung erkannt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Warnungen bei KeyArmor Aktivität	500000	VirusDefense	KeyArmor
Warnungen bei KeyArmor Aktivität	500001	Objekt gesäubert	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	500002	Objekt desinfiziert	KeyArmor
Warnungen bei KeyArmor Aktivität	500003	Objekt in Quarantäne	KeyArmor
Warnungen bei KeyArmor Aktivität	500004	Objekt gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	500005	Virus entdeckt	KeyArmor
Warnungen bei KeyArmor Aktivität	500006	Vollständige Suche gestartet	KeyArmor
Warnungen bei KeyArmor Aktivität	500007	Vollständige Suche abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500008	Objekt verdächtig	KeyArmor
Warnungen bei KeyArmor Aktivität	500009	Objektsuche abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500010	Suche auf Wechselmedium angefordert	KeyArmor
Warnungen bei KeyArmor Aktivität	500011	Suche auf Wechselmedium abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500012	Suche in Ordner angefordert	KeyArmor
Warnungen bei KeyArmor Aktivität	500013	Suche in Ordner abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500014	Zugriff auf Objekt verweigert	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	500015	Objekt beschädigt	KeyArmor
Warnungen bei KeyArmor Aktivität	500016	Objekt sauber	KeyArmor
Warnungen bei KeyArmor Aktivität	500017	Vollständige Suche abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500018	Suche in Objekt abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500019	Suche auf Wechselmedium abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500020	Suche in Ordner abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500021	Update gestartet	KeyArmor
Warnungen bei KeyArmor Aktivität	500022	Das Update war nicht erfolgreich. Versuchen Sie es erneut.	KeyArmor
Warnungen bei KeyArmor Aktivität	500023	Update abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500024	Update erfolgreich.	KeyArmor
Warnungen bei KeyArmor Aktivität	500025	VirusDefense auf dem neuesten Stand	KeyArmor
Warnungen bei KeyArmor Aktivität	500026	PalmVirusDefense	KeyArmor
Warnungen bei KeyArmor Aktivität	500027	Suche in Objekt angefordert	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	500028	PPCVirusDefense	KeyArmor
Warnungen bei KeyArmor Aktivität	900000	Angemeldeter Benutzer verwendet Einmalkennwort.	KeyArmor
Warnungen bei KeyArmor Aktivität	900001	Angemeldeter Benutzer verwendet festes Kennwort.	KeyArmor
Warnungen bei KeyArmor Aktivität	900002	Angemeldeter Benutzer verwendet Smartcard.	KeyArmor
Warnungen bei KeyArmor Aktivität	900003	Angemeldeter Benutzer verwendet Domänenauthentifizierung.	KeyArmor
Warnungen bei KeyArmor Aktivität	900004	Angemeldeter Benutzer verwendet Remote-Authentifizierung.	KeyArmor
Warnungen bei KeyArmor Aktivität	900005	Angemeldeter Benutzer verwendet ColorCode-Authentifizierung.	KeyArmor
Warnungen bei KeyArmor Aktivität	900006	Angemeldeter Benutzer verwendet PIN.	KeyArmor
Warnungen bei KeyArmor Aktivität	900007	Angemeldeter Benutzer verwendet OCSP	KeyArmor
Warnungen bei KeyArmor Aktivität	900008	Angemeldeter Benutzer verwendet Selbsthilfe.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	900009	Angemeldeter Benutzer verwendet RSA	KeyArmor
Warnungen bei KeyArmor Aktivität	900150	Anmelden des Benutzers mit Einmalkennwort ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900151	Anmelden des Benutzers mit festem Kennwort ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900152	Anmelden des Benutzers mit Smartcard ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900153	Anmelden des Benutzers mit Domänenauthentifizierung ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900154	Anmelden des Benutzers mit Remote-Authentifizierung ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900155	Anmelden des Benutzers mit ColorCode-Authentifizierung ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900156	Anmelden des Benutzers mit PIN ist fehlgeschlagen.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	900157	Anmelden des Benutzers mit OCSP ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900158	Benutzer wurde nach zu vielen fehlgeschlagenen Anmeldeversuchen gesperrt.	KeyArmor
Warnungen bei KeyArmor Aktivität	900301	Anzahl fehlgeschlagener Anmeldeversuche überschritten	KeyArmor
Warnungen bei KeyArmor Aktivität	900350	Schlüssel per Wipe gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	903000	Benutzer hat eine Datei umbenannt	KeyArmor
Warnungen bei KeyArmor Aktivität	903001	Benutzer hat eine Datei geändert	KeyArmor
Warnungen bei KeyArmor Aktivität	903002	Benutzer hat eine Datei gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	903003	Benutzer hat eine Datei erstellt	KeyArmor
Warnungen bei KeyArmor Aktivität	903100	Primäraktion erzwungen, da keine PolicyServer Verbindung besteht.	KeyArmor
Warnungen bei KeyArmor Aktivität	903101	Sekundäraktion erzwungen, da keine PolicyServer Verbindung besteht.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	903102	Richtlinien-Updates angewendet	KeyArmor
Warnungen bei KeyArmor Aktivität	904000	Infizierte Datei repariert	KeyArmor
Warnungen bei KeyArmor Aktivität	904001	Reparieren der infizierten Datei nicht möglich.	KeyArmor
Warnungen bei KeyArmor Aktivität	904002	Infizierte Datei wird übersprungen, Reparatur wird nicht unterstützt	KeyArmor
Warnungen bei KeyArmor Aktivität	904003	Infizierte Datei gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	904004	Löschen der infizierten Datei nicht möglich.	KeyArmor
Warnungen bei KeyArmor Aktivität	904005	Gerät wird auf Grund infizierter Datei ausgelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	904006	Fehler beim Auslöschen des Geräts auf Grund infizierter Datei	KeyArmor
Warnungen bei KeyArmor Aktivität	904007	Fallback-Aktion für infizierte Datei wird aufgerufen	KeyArmor
Warnungen bei KeyArmor Aktivität	904010	Antivirus-Dateien aktualisiert	KeyArmor
Warnungen bei KeyArmor Aktivität	904011	Antivirus-Dateien können nicht aktualisiert werden.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100013	Fehlgeschlagener Anmeldeversuch	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100014	Erfolgreiche Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100016	Anmeldung nicht möglich. Verwenden Sie die Remote-Authentifizierung, um den PolicyServer Administrator mit einem Herausforderungscode zu versehen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100021	Erfolglose ColorCode-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100022	Erfolglose Anmeldung per festem Kennwort	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100023	Erfolglose PIN-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100024	Erfolglose X99-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100028	Erfolgreiche ColorCode-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100031	Erfolgreiche X9.9-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100032	Erfolgreiche Remote-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100035	Erfolgreiche WebToken-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100036	Erfolglose WebToken-Anmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100050	Anmeldung mit festem Kennwort durch Sperre blockiert.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100051	Benutzeranmeldung entsperrt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100057	LDAP-Benutzerauthentifizierung erfolgreich	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100058	LDAP-Benutzerauthentifizierung fehlgeschlagen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100059	Änderung des LDAP-Benutzerkennworts erfolgreich	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100060	Änderung des LDAP-Benutzerkennworts fehlgeschlagen	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100061	Zugriffsanforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100070	Erfolgreiche Abmeldung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100433	Die eingegebenen ColorCode-Kennwörter stimmen nicht überein.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100434	ColorCode kann nicht geändert werden. Der neue ColorCode muss sich vom aktuellen unterscheiden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100435	ColorCode kann nicht geändert werden. Der neue ColorCode muss die von PolicyServer definierten Mindestanforderungen für die Länge erfüllen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100436	ColorCode kann nicht geändert werden. Der neue ColorCode muss sich von allen zuvor verwendeten ColorCodes unterscheiden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100437	Ändern des ColorCode fehlgeschlagen - Interner Fehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100459	X9.9 - Fehler bei Kennwortänderung - Verbindung zu PolicyServer Host nicht möglich	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100460	X9.9 - Fehler bei Kennwortänderung - Leere Seriennummer	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100461	X9.9 - Fehler bei Kennwortänderung - Interner Fehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	101004	Gesperrtes Gerät kann nicht zurückgesetzt werden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	104000	Smartcard-Anmeldung erfolgreich.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	104001	Smartcard-Anmeldung nicht erfolgreich. Prüfen Sie, ob die Karte ordnungsgemäß eingelegt wurde und die Smartcard-PIN gültig ist.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100037	Palm-Richtliniendatenbank fehlt	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100038	Fehler bei Palm-Verschlüsselung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100039	PPC - Geräteverschlüsselung geändert	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100040	PPC - Fehler bei Verschlüsselung	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Warnungen bei MobileFirewall-Aktivität	300000	MobileFirewall	MobileFirewall
Warnungen bei MobileFirewall-Aktivität	300001	DenialOfServiceAttack	MobileFirewall

Kategorie	Nachrichten -ID	Beschreibung	Produkte
OCSP-Warnungen	104005	OCSP-Zertifikatsstatus gut.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
OCSP-Warnungen	104006	OCSP-Zertifikatsstatus widerrufen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
OCSP-Warnungen	104007	OCSP-Zertifikatsstatus unbekannt.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
OTA-Warnungen	100041	OTA-Objekt fehlt oder ist beschädigt.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
OTA-Warnungen	100042	OTA-Synchronisierung erfolgreich	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
OTA-Warnungen	100043	OTA-Gerät ausgelöscht	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100017	Fehler beim Ändern des Kennworts	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Kennwortwarnungen	100018	Anzahl der Versuche zur Kennworteingabe überschritten	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100025	Kennwort zurückgesetzt auf 'ColorCode'	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100026	Kennwort zurückgesetzt auf 'Fest'	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100027	Kennwort zurückgesetzt auf PIN	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100029	Erfolgreiche Anmeldung per festem Kennwort	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100030	Erfolgreiche Anmeldung per PIN-Kennwort	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100033	Kennwort kann nicht zurückgesetzt werden	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Kennwortwarnungen	100432	Das Kennwort kann nicht geändert werden. Das neue Kennwort muss sich vom aktuellen Kennwort unterscheiden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100439	Das Kennwort kann nicht geändert werden. Die Kennwörter stimmen nicht überein.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100441	Das Kennwort kann nicht geändert werden. Das Kennwortfeld muss ausgefüllt werden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100442	Das Kennwort kann nicht geändert werden. Das Kennwort erfüllt nicht die von PolicyServer definierten Mindestanforderungen für die Länge.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100443	Das Kennwort kann nicht geändert werden. Ziffern sind nicht zulässig.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100444	Das Kennwort kann nicht geändert werden. Buchstaben sind nicht zulässig.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Kennwortwarnungen	100445	Das Kennwort kann nicht geändert werden. Sonderzeichen sind nicht zulässig.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100446	Das Kennwort kann nicht geändert werden. Das Kennwort darf den Benutzernamen nicht enthalten.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100447	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Sonderzeichen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100448	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Ziffern.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100449	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Zeichen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100450	Das Kennwort kann nicht geändert werden. Das Kennwort enthält zu viele aufeinanderfolgende Zeichen.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Kennwortwarnungen	100451	Das Kennwort kann nicht geändert werden. Das neue Kennwort muss sich von allen zuvor verwendeten Kennwörtern unterscheiden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100452	Ändern des Kennworts fehlgeschlagen - Interner Fehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	101003	Festes Kennwort wurde geändert.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	700100	Kennwort auf festes Kennwort zurückgesetzt.	File Encryption SP6 oder früher
Kennwortwarnungen	700101	Kennwort auf Smartcard zurückgesetzt.	File Encryption SP6 oder früher
Kennwortwarnungen	700102	Kennwort auf Domänenauthentifizierung zurückgesetzt.	File Encryption SP6 oder früher
Kennwortwarnungen	900159	Das Kennwort kann nicht geändert werden.	KeyArmor
Kennwortwarnungen	900160	Das Kennwort wurde erfolgreich geändert.	KeyArmor

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Kennwortwarnungen	900302	Kennwort auf festes Kennwort zurückgesetzt.	KeyArmor
Kennwortwarnungen	900303	Kennwort auf Smartcard zurückgesetzt.	KeyArmor
Kennwortwarnungen	900304	Kennwort auf Domänenauthentifizierung zurückgesetzt.	KeyArmor
PIN-Änderungswarnungen	100438	PIN kann nicht geändert werden. Die PINs stimmen nicht überein.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100440	PIN kann nicht geändert werden. Eines der Felder ist leer.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100453	PIN kann nicht geändert werden. Die PINs stimmen nicht überein.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100454	Änderung der PIN möglich. Die neue PIN muss sich von der alten PIN unterscheiden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
PIN-Änderungswarnungen	100455	PIN kann nicht geändert werden. Die neue PIN erfüllt nicht die von PolicyServer definierten Mindestanforderungen für die Länge.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100456	PIN kann nicht geändert werden. Die PIN darf den Benutzernamen nicht enthalten.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100457	PIN kann nicht geändert werden. Die neue PIN muss sich von allen zuvor verwendeten PINs unterscheiden.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100458	Ändern der PIN fehlgeschlagen - Interner Fehler	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Smartcard-Warnungen	104002	Registrierte Smartcard.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten -ID	Beschreibung	Produkte
Smartcard-Warnungen	104004	Smartcard kann nicht registriert werden. Prüfen Sie, ob die Karte ordnungsgemäß eingelegt wurde und die Smartcard-PIN gültig ist.	Full Disk Encryption, File Encryption, DriveArmor, KeyArmor oder PolicyServer
Windows Mobile Warnungen	800000	OTA-Installation gestartet	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800001	OTA-Installation abgeschlossen	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800100	OTA-SMS-Nachricht gesendet	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800200	OTA-Verzeichnisliste empfangen	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800300	OTA-Geräteattribute empfangen	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800400	OTA-Gerätesicherung	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800500	OTA-Gerätewiederherstellung	Full Disk Encryption für Windows Mobile

Anhang C

Endpoint Encryption Dienste

In der folgenden Tabelle werden alle Endpoint Encryption Dienste beschrieben. Die Informationen vermitteln ein Verständnis darüber, welche Dienste welche Endpoint Encryption Agents bzw. Funktion steuern und wie Sie ein Problem lösen.

TABELLE C-1. Endpoint Encryption Dienste

BETRIEBSSYSTEM	DIENST- ODER DAEMON-NAMEN	ANZEIGENAME	BESCHREIBUNG	DATEINAME
PolicyServer	PolicyServer Windows-Dienst	PolicyServer Windows-Dienst	Verwaltet die Kommunikation zwischen Endpoint Encryption Diensten und Datenbanken.	`PolicyServerWindowService.exe`
	TMEE Dienst	Endpoint Encryption Dienst	Verwaltet die Kommunikation zwischen Endpoint Encryption Agent 5.0 (und höher) über einen verschlüsselten Kanal (RESTful).	`TMEEService.exe`
	IIS/ MAWebService2	Legacy Web-Service	Verwaltet die Kommunikation zwischen Endpoint Encryption Agent 3.1.3 (und älter) über einen verschlüsselten Kanal (SOAP).	n. v.
	TMEEForward	TMEEForward	Leitet den Datenverkehr von Endpoint Encryption 5.0 Patch 1 Agents zu PolicyServer weiter.	TMEEForward.exe
	TMEEProxyWindowsService	PolicyServer LDAProxy-Windows-Dienst	Bietet sichere Kommunikation zwischen Trend Micro PolicyServer und den Remote-LDAP-Servern.	`LDAProxyWindowsServices.exe`

Betriebssystem	Dienst- oder Daemon-Namen	Anzeigename	Beschreibung	Dateiname
Full Disk Encryption	DrAService	Trend Micro Full Disk Encryption	Bietet Sicherheit für Trend Micro Endpoint und die Verschlüsselung ganzer Festplatten.	`DrAService.exe`
Encryption Management for Microsoft BitLocker	FDE_MB	Trend Micro Full Disk Encryption, Encryption Management for Microsoft BitLocker	Gewährleistet Datensicherheit für Endpunkte mit Microsoft BitLocker	`FDEforBitLocker.exe`
Encryption Management for Apple FileVault	Daemon: TMFDEMM Agent: Trend Micro Full Disk Encryption	Trend Micro Full Disk Encryption, Encryption Management for Apple FileVault	Gewährleistet Datensicherheit für Endpunkte mit Apple FileVault.	
File Encryption	FileEncryption Service	Trend Micro File Encryption	Gewährleistet Trend Micro Endpunktsicherheit und Datenschutz für Dateien, Ordner und Wechselmedien.	`FEService.exe`

Anhang D

Richtlinienzuordnung zwischen Management-Konsolen

Administratoren können Endpoint Encryption nur mit PolicyServer MMC verwalten, oder sie verwalten Endpoint Encryption mit Control Manager zur Verwaltung von Richtlinien, Benutzern und Geräten und setzen PolicyServer MMC für die erweiterte Protokollverwaltung und Berichterstellung ein.

In den folgenden Tabellen wird beschrieben, wie Richtlinien zwischen PolicyServer MMC und Control Manager zugeordnet werden. In Umgebungen, in denen Control Manager zur Verwaltung von PolicyServer eingesetzt wird, sollten Sie alle Richtlinien, die nicht in der Tabelle aufgeführt werden, mit PolicyServer MMC verwalten.

TABELLE D-1. Richtlinienzuordnung für Full Disk Encryption

CONTROL MANAGER BEZEICHNUNG	POLICYSERVER MMC PFAD
Verschlüsselung	
Endpunkt verschlüsseln	**Full Disk Encryption** > **Verschlüsselung** > **Gerät verschlüsseln**
Client-Einstellungen	
Full Disk Encryption Preboot umgehen	**Full Disk Encryption** > **Anmelden** > **Preboot-Umgehung**

Control Manager Bezeichnung	PolicyServer MMC Pfad
Benutzer sind berechtigt, auf die Systemwiederherstellungstools des Geräts zuzugreifen	**Full Disk Encryption** > **Agent** > **Wiederherstellung durch Benutzer zulassen**
Benachrichtigungen	
Die folgende Meldung wird angezeigt, wenn der Endpunkt gefunden wird	**Full Disk Encryption** > **Anmelden** > **Falls gefunden**
Die Kontaktinformationen für den technischen Support werden angezeigt	**Full Disk Encryption** > **Anmelden** > **Support-Informationen**
Rechtlichen Hinweis anzeigen	**Full Disk Encryption** > **Anmelden** > **Rechtlicher Hinweis**
• **Rechtlichen Hinweis anzeigen** > **Installation** • **Rechtlichen Hinweis anzeigen** > **Start**	**Full Disk Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Rechtlicher Hinweis** > **Anzeigezeit für den rechtlichen Hinweis**
Rechtlichen Hinweis anzeigen	**Full Disk Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Rechtlicher Hinweis** > **Text des rechtlichen Hinweises**

Tabelle D-2. Richtlinienzuordnung für File Encryption

Control Manager Bezeichnung	PolicyServer MMC Pfad
Zu verschlüsselnde Ordner	
Zu verschlüsselnde Ordner Textfeld	**File Encryption** > **Verschlüsselung** > **Ordner zum Verschlüsseln angeben**
Verwendeter Verschlüsselungsschlüssel	
Verwendeter Verschlüsselungsschlüssel	**File Encryption** > **Verschlüsselung** > **Verwendeter Verschlüsselungsschlüssel**

Control Manager Bezeichnung	PolicyServer MMC Pfad
Speichereinheiten	
Optisches Laufwerk deaktivieren	**File Encryption** > **Verschlüsselung** > **Optisches Laufwerk deaktivieren**
USB-Laufwerk deaktivieren	**File Encryption** > **Verschlüsselung** > **Wechselmedien** > **USB-Laufwerk deaktivieren**
Alle Dateien und Ordner auf USB-Laufwerken verschlüsseln	**File Encryption** > **Verschlüsselung** > **Wechselmedien** > **Gerät vollständig verschlüsseln**
Zu verschlüsselnden Dateipfad auf USB-Geräten angeben	**File Encryption** > **Verschlüsselung** > **Wechselmedien** > **Zu verschlüsselnde Ordner auf Wechselmedien**
Benachrichtigungen	
Rechtlichen Hinweis anzeigen	**File Encryption** > **Anmelden** > **Rechtlicher Hinweis**
• **Rechtlichen Hinweis anzeigen** > **Installation** • **Rechtlichen Hinweis anzeigen** > **Start**	**File Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Anzeigezeit für den rechtlichen Hinweis**
Rechtlichen Hinweis anzeigen Textfeld	**File Encryption** > **Anmelden** > **Rechtlicher Hinweis** > **Text des rechtlichen Hinweises**

Tabelle D-3. Allgemeine Richtlinienzuordnung

Control Manager Bezeichnung	PolicyServer MMC Pfad
Deinstallation durch Benutzer zulassen	
Nicht-Administratorkonten können die Agent-Software deinstallieren	• **Full Disk Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen** • **File Encryption** > **Agent** > **Deinstallation durch Benutzer zulassen**

CONTROL MANAGER BEZEICHNUNG	POLICYSERVER MMC PFAD
Aktionen zum Sperren von Geräten	
Konto sperren nach *<number>* Tagen	**Full Disk Encryption** > **Anmelden** > **Zeitraum bis Kontosperrung**
Kontosperraktion	**Full Disk Encryption** > **Anmelden** > **Kontosperraktion**
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	**Full Disk Encryption** > **Anmelden** > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**
Full Disk Encryption: **Aktion zur Gerätesperrung**	**Full Disk Encryption** > **Anmelden** > **Aktion zur Gerätesperrung**
Full Disk Encryption: **Anzahl der Minuten, die das Gerät gesperrt wird**	**Full Disk Encryption** > **Anmelden** > **Zeitverzögerung bei Gerätesperre**
File Encryption: **Aktion zur Gerätesperrung**	**File Encryption** > **Anmelden** > **Aktion zur Gerätesperrung**
File Encryption: **Anzahl der Minuten, die das Gerät gesperrt wird**	**File Encryption** > **Anmelden** > **Zeitverzögerung bei Gerätesperre**
Kennwort	
Benutzer muss das Kennwort nach *<number>* Tagen ändern	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Kennwort ändern alle**
Benutzer darf die vorherigen *<number>* Kennwörter nicht wiederverwenden	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Aufbewahrung des Kennwortverlaufs**
Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Zulässige aufeinanderfolgende Zeichen**

CONTROL MANAGER BEZEICHNUNG	POLICYSERVER MMC PFAD
Zulässige Mindestlänge für Kennwörter	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Mindestlänge**
Anforderungen an die Zeichen für Kennwörter	
Buchstaben	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Zeichen**
Kleinbuchstaben	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Kleinbuchstaben**
Großbuchstaben	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Großbuchstaben**
Zahlen	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Ziffern**
Symbole	**Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Benutzerkennwort** > **Erforderliche Anzahl an Sonderzeichen**

Anhang E

Integration von OfficeScan

Im Folgenden wird beschrieben, wie das OfficeScan Plug-in für das Endpoint Encryption Verteilungstool zur Verteilung von Endpoint Encryption in Unternehmen mit Endpunkten, die von OfficeScan verwaltet werden, verwendet wird.

Informationen über die Voraussetzungen für PolicyServer, die Systemvoraussetzungen für OfficeScan und die Verwaltung des Plug-in für das Endpoint Encryption Verteilungstool finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Es werden folgende Themen behandelt:

- *Info über Trend Micro OfficeScan Integration auf Seite E-2*
- *Info über den Plug-in Manager auf Seite E-3*
- *Plug-in-Programme verwenden auf Seite E-5*
- *Die OfficeScan Agent-Hierarchie auf Seite E-5*
- *Verteilung von Endpoint Encryption Agents auf Seite E-10*

Info über Trend Micro OfficeScan Integration

OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet. Der Agent überwacht den Endpunkt und sendet dessen Sicherheitsstatus an den Server. Über die webbasierte Management-Konsole vereinfacht der Server das Festlegen koordinierter Sicherheitsrichtlinien und verteilt Updates an alle Agents.

Hinweis

Informationen über OfficeScan finden Sie in der Begleitdokumentation unter:

http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool können Sie die Endpoint Encryption Agents auf verwaltete OfficeScan Endpunkte verteilen. Sie können Endpunkte auf Grundlage bestimmter Kriterien auswählen und den Status der Verteilung anzeigen. Nachdem das Plug-in für das Endpoint Encryption Verteilungstool die Software für den Endpoint Encryption Agent verteilt hat, führt der Endpoint Encryption Agent eine Synchronisierung mit PolicyServer unter Verwendung der Einstellungen durch, die im Plug-in angegeben wurden. OfficeScan verwaltet keine Endpoint Encryption Richtlinien. Der OfficeScan Agent und der Endpoint Encryption Agent befinden sich unabhängig voneinander auf demselben Endpunkt.

In der folgenden Darstellung wird illustriert, wie Sie Endpoint Encryption zum ersten Mal auf Endpunkte verteilen, die von OfficeScan verwaltet werden. In OfficeScan

Installationen können Administratoren PolicyServer entweder mit Control Manager oder PolicyServer MMC verwalten.

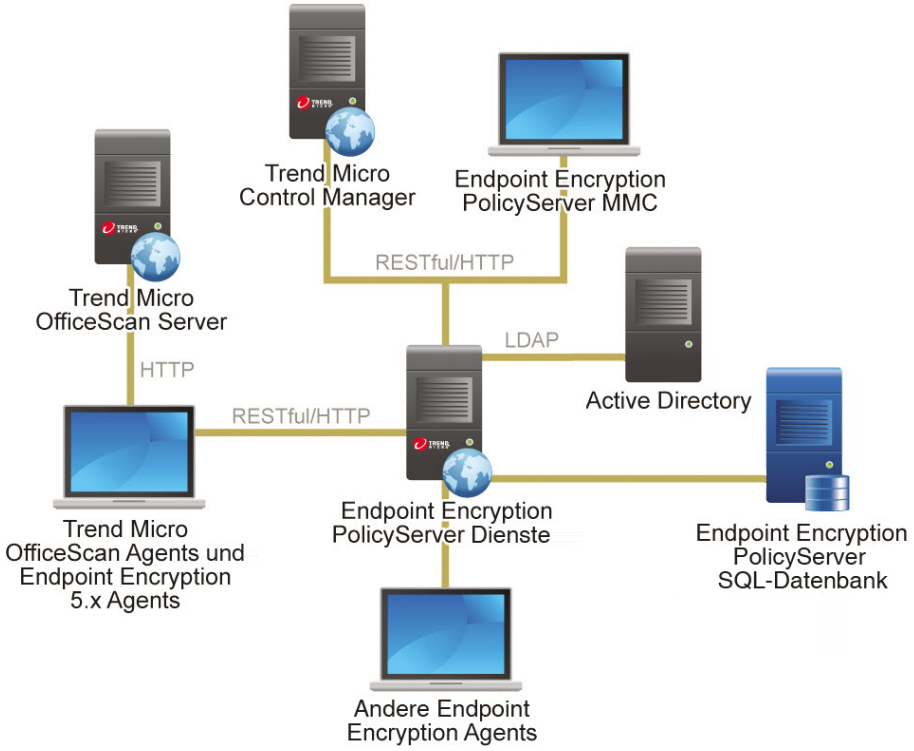


ABBILDUNG E-1. Verteilung der OfficeScan Integration

Info über den Plug-in Manager

OfficeScan umfasst ein Framework mit der Bezeichnung Plug-in Manager, das neue Lösungen in die bestehende OfficeScan Umgebung integriert. Um die Verwaltung dieser Lösungen zu vereinfachen, stellt Plug-in Manager die Daten dieser Lösungen in Form von Widgets übersichtlich dar.

Hinweis

Keine der Plug-in-Lösungen unterstützt zurzeit IPv6. Der Server kann diese Lösungen zwar herunterladen, er kann sie aber nicht auf reine IPv6 Endpoint Encryption Agents oder reine IPv6-Hosts verteilen.

Plug-in Manager liefert zwei verschiedene Lösungen:

- **Native Produktfunktionen**

  Einige native OfficeScan Funktionen werden über Plug-in Manager separat lizenziert und aktiviert. In dieser Version fallen zwei Funktionen unter diese Kategorie, nämlich **Trend Micro Virtual Desktop Support** und **OfficeScan Datentschutz**.

- **Plug-in-Programme**

  Plug-in-Programme sind nicht Teil des OfficeScan Programms. Die Plug-in-Programme haben separate Lizenzen und Management-Konsolen. Greifen Sie auf die Management-Konsolen über die OfficeScan Webkonsole zu. Beispiele für Plug-in-Programme sind **Intrusion Defense Firewall**, **Trend Micro Security (für Mac)** und **Trend Micro Mobile Security**.

Diese Dokumente geben einen allgemeinen Überblick über Installation und Verwaltung von Plug-in-Programmen und erklären die in Widgets dargestellten Informationen über die Plug-in-Programme. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

OfficeScan installieren

Informationen zur Installation und Konfiguration von OfficeScan finden Sie in der Dokumentation, die Sie unter der folgenden Adresse herunterladen können:

http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Informationen zu den Installations- und Konfigurationsoptionen des OfficeScan Endpoint Encryption Verteilungstools vor der Verteilung der Endpoint Encryption Agents finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Plug-in-Programme verwenden

In diesem Abschnitt wird beschrieben, wie Sie das Plug-in-Programm für das OfficeScan Endpoint Encryption Verteilungstool installieren und verwalten.

Verwaltung der Plug-in-Programme

Konfigurieren Sie die Einstellungen und führen Sie programmbezogene Aufgaben über die Management-Konsole des Plug-in-Programms durch, auf die Sie über die OfficeScan Webkonsole zugreifen können. Zu den Aufgaben gehören das Aktivieren des Programms und die mögliche Verteilung des Plug-in-Programm-Agents an die Endpunkte. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

Endpoint Encryption Verteilungstool verwalten

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-in Manager**.
2. Navigieren Sie im **Plug-in Manager** Fenster zum Abschnitt für Plug-in-Programme, und klicken Sie auf **Programm verwalten**.

Die OfficeScan Agent-Hierarchie

In der OfficeScan Agent-Hierarchie werden alle Agents – in OfficeScan Domänen gruppiert – angezeigt, die gegenwärtig vom Server verwaltet werden. Agents werden in Domänen gruppiert, so dass Sie für alle Domänenmitglieder gleichzeitig dieselbe Konfiguration festlegen, verwalten und übernehmen können.

Spezifische Aufgaben in der Agent-Hierarchie

Die Agent-Hierarchie wird angezeigt, wenn Sie bestimmte Fenster auf der Webkonsole öffnen. Oberhalb der Agent-Hierarchie befinden sich Menübefehle, die sich auf das gerade geöffnete Fenster beziehen. Mit Hilfe dieser Menübefehle können Sie bestimmte Aufgaben ausführen, z. B. die Konfiguration der Agent-Einstellungen oder die Einleitung von Agent-Aufgaben. Um eine dieser Aufgaben durchzuführen, wählen Sie zunächst ein Ziel für die Aufgabe, und wählen Sie anschließend einen Menübefehl.

Die Agent-Hierarchie bietet den Zugriff auf die folgenden Funktionen:

- **Nach Endpunkten suchen:** Suchen Sie nach bestimmten Endpunkten, indem Sie Suchkriterien in das Textfeld eingeben.
- **Mit OfficeScan synchronisieren**: Synchronisieren Sie die Agent-Hierarchie des Plug-in-Programms mit der Agent-Hierarchie von OfficeScan Server. Weitere Informationen finden Sie unter *Agent-Hierarchie synchronisieren auf Seite E-6*.
- **Server-Einstellungen verteilen**: Zeigt das Fenster **Server-Einstellungen verteilen** an. Weitere Informationen finden Sie unter *Servereinstellungen verteilen auf Seite E-10*.

Administratoren können auch die Agent-Hierarchie manuell durchsuchen, um Endpunkte oder Domänen zu finden. Die computerspezifischen Informationen werden in der Tabelle rechts angezeigt.

Agent-Hierarchie synchronisieren

Bevor das Plug-in-Programm die Einstellungen an die Agents verteilen kann, müssen Administratoren die Agent-Hierarchie mit dem OfficeScan Server synchronisieren.

Prozedur

1. Öffnen Sie die Plug-in-Konsole.
2. Klicken Sie im Fenster **Client-Verwaltung** auf **Mit OfficeScan synchronisieren**.

   Ein Bestätigungsfenster wird angezeigt.
3. Warten Sie, bis der Synchronisierungsvorgang abgeschlossen ist.

4. Klicken Sie auf **Schließen**, um zum Fenster **Client-Verwaltung** zurückzukehren.

Fehlercodes bei der Installation von Endpoint Encryption Agents

In der folgenden Tabelle werden die Fehlercodes für Fehler bei der Installation von Endpoint Encryption Agents beschrieben. Anhand dieser Tabelle können Sie das Problem verstehen und eine Lösung für den jeweiligen Installationsfehler finden.

Hinweis

Vergewissern Sie sich vor der Verteilung der Endpoint Encryption Agents, dass der Endpunkt die minimalen Systemvoraussetzungen erfüllt. Microsoft .NET Framework 2.0 SP1 oder höher ist erforderlich. Informationen zu den Systemvoraussetzungen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

TABELLE E-1. Fehlercodes im Zusammenhang mit der Installation

AGENT	FEHLERCODE	PROBLEM UND LÖSUNG
File Encryption	1603	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.

AGENT	FEHLERCODE	PROBLEM UND LÖSUNG
Full Disk Encryption	-3	Der Benutzername oder das Kennwort ist ungültig. Überprüfen Sie die Anmeldedaten, und melden Sie sich erneut am PolicyServer an.
	-6	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
	-13	Der Endpunkt erfüllt nicht die minimalen Systemvoraussetzungen. Rüsten Sie den Arbeitsspeicher oder den Festplattenspeicherplatz auf, und wiederholen Sie die Installation des Agent.

AGENT	FEHLERCODE	PROBLEM UND LÖSUNG
Encryption Management for Microsoft BitLocker	1603	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
	-13	Der Endpoint Encryption Agent kann nicht installiert werden. Microsoft BitLocker erfordert das TPM-Sicherheitsgerät (Trusted Platform Module). Der Endpunkt unterstützt entweder TPM nicht, oder TPM ist nicht im BIOS aktiviert, oder TPM ist durch einen anderen angemeldeten Benutzer gesperrt. Aktivieren Sie TPM im BIOS, oder wenden Sie sich an den Systemadministrator.
	-14	Der Endpoint Encryption Agent kann nicht installiert werden. Das Betriebssystem wird nicht unterstützt. Installieren Sie eines der folgenden unterstützten Betriebssysteme, und versuchen Sie es anschließend erneut: • Windows 7, 32 Bit oder 64 Bit, Ultimate oder Enterprise Edition • Windows 8, 32 Bit oder 64 Bit, Professional oder Enterprise Edition
	-15	Full Disk Encryption ist bereits installiert.
	-16	Der Endpoint Encryption Agent kann nicht installiert werden. Der Endpunkt ist bereits verschlüsselt.

Servereinstellungen verteilen

Sie können die Einstellungen für PolicyServer konfigurieren und verteilen, um die Kommunikation zwischen den Agents und PolicyServer sicherzustellen.

Prozedur

1. Öffnen Sie die Plug-in-Programmkonsole.
2. Klicken Sie auf die Registerkarte **PolicyServer Einstellungen**.
3. Geben Sie die folgenden Details an:

Option	Bezeichnung
Servername:	Geben Sie die IP-Adresse oder den Host-Namen für den PolicyServer ein.
Port	Geben Sie die Portnummer an, die der PolicyServer Instanz zugewiesen wurde.
Unternehmen	Geben Sie das PolicyServer Unternehmen an. Nur ein Unternehmen wird unterstützt.
Benutzername	Geben Sie den Benutzernamen für den Unternehmensadministrator an.
Kennwort	Geben Sie das Kennwort für den Unternehmensadministrator an.

4. Klicken Sie auf **Speichern**.

   Eine Bestätigungsmeldung wird angezeigt. Warten Sie, bis die Verbindung mit dem Server erstellt wurde.

Verteilung von Endpoint Encryption Agents

In diesem Abschnitt wird beschrieben, wie Sie mit dem Plug-in für das Endpoint Encryption Verteilungstool die Befehle zur Installation und Deinstallation von Agents einleiten.

Die folgende Darstellung zeigt das Endpoint Encryption Verteilungstool-Fenster **Client-Verwaltung**.

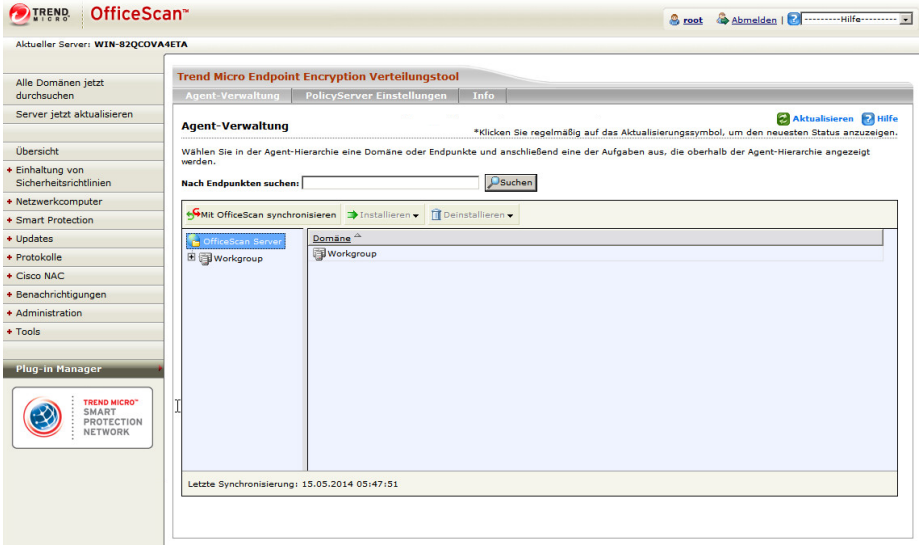


ABBILDUNG E-2. Endpoint Encryption - Verteilungstool

Agent mit OfficeScan verteilen

Vergewissern Sie sich vor der Verteilung von Agents, dass die Endpunkte die minimalen Systemvoraussetzungen erfüllen.Weitere Informationen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Prozedur

1. Wählen Sie den Endpunkt in der Client-Hierarchie aus.

Hinweis

Wenn Sie mehrere Endpunkte auswählen möchten, halten Sie die STRG-Taste gedrückt, und wählen Sie die entsprechenden Endpunkte aus.

2. Klicken Sie auf **Installieren**, und wählen Sie anschließend eine der folgenden Optionen:

Option	Bezeichnung
Full Disk Encryption	Wählen Sie die entsprechenden Full Disk Encryption Agents. • Wählen Sie den Full Disk Encryption Agent, um alle Funktionen zu verteilen, einschließlich Preboot-Authentifizierung, aller Richtlinien, Benachrichtigungen und Aktionen für Geräte. • Wählen Sie den Agent für die Encryption Management for Microsoft BitLocker, um die Festplattenverschlüsselung von Microsoft BitLocker zu aktivieren. Dabei werden nur begrenzte Richtlinien und Aktionen für Geräte verteilt. **Hinweis** Es ist nicht möglich, den Agent der Encryption Management for Apple FileVault mit dem Endpoint Encryption Verteilungstool Plug-in zu verteilen.
File Encryption	Bei der Verteilung von File Encryption Agent sind alle Funktionen und Richtlinien enthalten.

3. Klicken Sie auf **Verteilen**.

4. Wenn eine Meldung angezeigt wird, klicken Sie auf **OK**, um die Verteilung zu bestätigen.

Der Befehl für die Agent-Verteilung wird eingeleitet. Bei Erfolg wird die Aufforderung angezeigt, den ausgewählten Endpunkt neu zu starten.

Agent-Verteilung bestätigen

Mit dieser Aufgabe wird erklärt, wie Sie bestätigen, dass die Installation von Endpoint Encryption Agent auf dem Endpunkt richtig initialisiert wurde.

Prozedur

1. Führen Sie *Agent mit OfficeScan verteilen auf Seite E-11* durch.

2. Melden Sie sich am ausgewählten Endpoint Encryption Gerät an.

3. Wählen Sie eine der folgenden Optionen:

   - Um den Status der Verteilung anzuzeigen, öffnen Sie die Protokolldateien unter:

     Client-Endpunkt

     `C:\TMEE_Deploy_Client.log`

     Server-Endpunkt

     `C:\TMEE_Deploy_Server_Inst.log`

   - Führen Sie den Task-Manager aus, und suchen Sie nach einem der Dienste unter *Endpoint Encryption Agent-Dienste auf Seite E-13*.

4. Sobald die Verteilung der Endpoint Encryption Agents beendet ist, starten Sie den Endpunkt neu, um die Installation abzuschließen.

Endpoint Encryption Agent-Dienste

In der folgenden Tabelle werden die Dienste beschrieben, die ausgeführt werden, wenn der Endpoint Encryption Agent auf dem Endpunkt initiiert wird. Anhand dieser Informationen können Sie überprüfen, ob der Agent erfolgreich installiert wurde und ordnungsgemäß funktioniert.

Hinweis

Weitere Informationen zu Endpoint Encryption Diensten finden Sie unter *Endpoint Encryption Dienste auf Seite C-1*.

DIENST	STATUS
`FEService.exe`	Der File Encryption Agent wird ausgeführt.
`TMFDE.exe`	Der Full Disk Encryption Agent wird ausgeführt.

Dienst	Status
`TMFDEForBitLocker.exe`	Die Encryption Management for Microsoft BitLocker Agent wird ausgeführt.

Statusangaben zur Verteilung von Endpoint Encryption Agents

In der folgenden Tabelle werden die Statusangaben von OfficeScan beschrieben, die auf der Konsole des Plug-ins für das Endpoint Encryption Verteilungstool nach der Initiierung des Verteilungsbefehls angezeigt werden. Anhand dieser Informationen können Sie ermitteln, ob während der Installation oder Deinstallation des Agents ein Problem aufgetreten ist.

Tabelle E-2. Statusangaben zur Agent-Installation

Status	Nachricht	Beschreibung
Wird ausgeführt	Wird ausgeführt: Agent-Verteilung	OfficeScan versucht, eine Kommunikation mit dem verwalteten Endpunkt aufzubauen, den Endpoint Encryption Agent zu installieren und dann eine Verbindung mit PolicyServer zu erstellen.
Erfolgreich	Erfolgreiche Verteilung des Agent	Der Endpoint Encryption Agent wurde erfolgreich installiert und konnte die Kommunikation mit OfficeScan und PolicyServer aufbauen.
Fehlgeschlagen	Erfolglose Verteilung des Agent	Die Verteilung des Endpoint Encryption Agent konnte nicht abgeschlossen werden. Ermitteln Sie anhand der Protokolle, warum der verwaltete Endpunkt nicht mit dem ausgewählten Endpoint Encryption Agent aktualisiert werden konnte.

Status	Nachricht	Beschreibung
Neustart erforderlich	Erfolgreiche Verteilung des Agent Herunterfahren/Neustart erforderlich.	Beim Full Disk Encryption Agent ist ein Neustart erforderlich, um die Installation abzuschließen. Der Status wird erst aktualisiert, nachdem sich der Benutzer bei PolicyServer Preboot angemeldet hat.
Zeitüberschreitung	Zeitüberschreitung: Agent-Verteilung	Der Zeitraum für die Zeitüberschreitung beträgt 30 Minuten. Initiieren Sie nach einer Zeitüberschreitung einen neuen Verteilungsbefehl.

Tabelle E-3. Statusangaben zur Agent-Deinstallation

Status	Nachricht	Beschreibung
Wird ausgeführt	Anforderung wird ausgeführt: Agent-Verteilung	OfficeScan versucht, mit dem verwalteten Endpunkt zu kommunizieren und die Agent-Software zu deinstallieren. Die Deinstallation kann erst starten, nachdem der verwaltete Endpunkt geantwortet hat.
Erfolgreich	Erfolgreiche Deinstallation des Agent	Der Endpoint Encryption Agent wurde erfolgreich deinstalliert und konnte die Kommunikation mit OfficeScan und PolicyServer aufbauen. Nach der Deinstallation wird das Endpoint Encryption Gerät von PolicyServer entfernt.
Fehlgeschlagen	Erfolglose Deinstallation des Agent	Für die Anforderung zur Deinstallation des Endpoint Encryption Agent konnte keine Verbindung erstellt werden. Ermitteln Sie anhand der Protokolle, warum auf dem verwalteten Endpunkt Endpoint Encryption nicht deinstalliert werden konnte.

STATUS	NACHRICHT	BESCHREIBUNG
Neustart erforderlich	Erfolgreiche Deinstallation des Agent Herunterfahren/Neustart erforderlich.	Einige Endpoint Encryption Agents müssen neu gestartet werden, damit die Deinstallation abgeschlossen werden kann.
Zeitüberschreitung	Zeitüberschreitung der Anforderung: Agent deinstallieren	Der Zeitraum für die Zeitüberschreitung beträgt 30 Minuten. Initiieren Sie nach einer Zeitüberschreitung einen neuen Deinstallationsbefehl.

Fehlercodes bei der Installation von Endpoint Encryption Agents

In der folgenden Tabelle werden die Fehlercodes für Fehler bei der Installation von Endpoint Encryption Agents beschrieben. Anhand dieser Tabelle können Sie das Problem verstehen und eine Lösung für den jeweiligen Installationsfehler finden.

Hinweis

Vergewissern Sie sich vor der Verteilung der Endpoint Encryption Agents, dass der Endpunkt die minimalen Systemvoraussetzungen erfüllt. Microsoft .NET Framework 2.0 SP1 oder höher ist erforderlich. Informationen zu den Systemvoraussetzungen finden Sie im *Endpoint Encryption Installations- und Migrationshandbuch*.

Tabelle E-4. Fehlercodes im Zusammenhang mit der Installation

Agent	Fehlercode	Problem und Lösung
File Encryption	1603	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
Full Disk Encryption	-3	Der Benutzername oder das Kennwort ist ungültig. Überprüfen Sie die Anmeldedaten, und melden Sie sich erneut am PolicyServer an.
	-6	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
	-13	Der Endpunkt erfüllt nicht die minimalen Systemvoraussetzungen. Rüsten Sie den Arbeitsspeicher oder den Festplattenspeicherplatz auf, und wiederholen Sie die Installation des Agent.

Agent	Fehlercode	Problem und Lösung
Encryption Management for Microsoft BitLocker	1603	Der Endpoint Encryption Agent kann nicht installiert werden. Möglicherweise ist eine erforderliche Ressource nicht verfügbar. Starten Sie den Endpunkt neu, und wiederholen Sie die Installation. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.
	-13	Der Endpoint Encryption Agent kann nicht installiert werden. Microsoft BitLocker erfordert das TPM-Sicherheitsgerät (Trusted Platform Module). Der Endpunkt unterstützt entweder TPM nicht, oder TPM ist nicht im BIOS aktiviert, oder TPM ist durch einen anderen angemeldeten Benutzer gesperrt. Aktivieren Sie TPM im BIOS, oder wenden Sie sich an den Systemadministrator.
	-14	Der Endpoint Encryption Agent kann nicht installiert werden. Das Betriebssystem wird nicht unterstützt. Installieren Sie eines der folgenden unterstützten Betriebssysteme, und versuchen Sie es anschließend erneut: • Windows 7, 32 Bit oder 64 Bit, Ultimate oder Enterprise Edition • Windows 8, 32 Bit oder 64 Bit, Professional oder Enterprise Edition
	-15	Full Disk Encryption ist bereits installiert.
	-16	Der Endpoint Encryption Agent kann nicht installiert werden. Der Endpunkt ist bereits verschlüsselt.

Mit OfficeScan Endpoint Encryption Agents deinstallieren

Während eines Upgrades ist es bei einigen Endpoint Encryption Agents erforderlich, zuerst die alte Software für die Endpoint Encryption Agents manuell zu deinstallieren. Wenn die Software des Endpoint Encryption Agent Fehlfunktionen zeigt, lässt sich das Problem möglicherweise durch Deinstallieren und erneutes Installieren der Software für den Endpoint Encryption Agent lösen. Dieses Verfahren erklärt die Deinstallation von Endpoint Encryption Agents mit dem Plug-in für das OfficeScan Endpoint Encryption Verteilungstool.

Prozedur

1. Wählen Sie das Endpoint Encryption Gerät.

   Hinweis

   Wenn Sie mehrere Endpoint Encryption Geräte auswählen möchten, halten Sie die UMSCHALTTASTE gedrückt, und wählen Sie die entsprechenden Endpunkte.

2. Klicken Sie auf **Deinstallieren**, und wählen Sie den entsprechenden Endpoint Encryption Agent aus dem Listenfeld.

3. Klicken Sie auf **OK**, um die Verteilung zu bestätigen.

   Der Deinstallationsbefehl für den Endpoint Encryption Agent wird verteilt.

4. Die Deinstallation des Endpoint Encryption Agent ist abgeschlossen, wenn OfficeScan die Bestätigungsmeldung anzeigt.

   Hinweis

   Alle zukünftigen Verteilungsbefehle schlagen fehl, wenn das Endpoint Encryption Gerät nicht neu gestartet wird, nachdem der Deinstallationsbefehl aufgerufen und abgeschlossen wurde. Wenn die Deinstallation nicht abgeschlossen werden kann, führen Sie die manuelle Deinstallation aus dem *Endpoint Encryption Installations- und Migrationshandbuch* durch.

Bei vollständiger Deinstallation wird der Endpoint Encryption Agent entfernt, und der Produktordner wird auf dem Endpunkt gelöscht.

Anhang F

Glossar

In der folgenden Tabelle wird die Terminologie beschrieben, die in der gesamten Endpoint Encryption Dokumentation verwendet wird.

TABELLE F-1. Endpoint Encryption Terminologie

BEGRIFF	BESCHREIBUNG
Agent	Software, die auf einem Endpunkt installiert ist und die mit einem Verwaltungsserver kommuniziert.
Authentifizierung	Der Prozess des Identifizierens eines Benutzers.
ColorCode™	Die Authentifizierungsmethode, bei der eine Farbfolge als Kennwort eingegeben werden muss.
Command Line Helper	Ein Trend Micro Tool zum Erstellen von verschlüsselten Werten, um die Anmeldedaten zu sichern, wenn Installationsskripts für Endpoint Encryption Agents erstellt werden.
Command Line Installer Helper	Ein Trend Micro Tool zum Erstellen von verschlüsselten Werten, um die Anmeldedaten zu sichern, wenn Installationsskripts für Endpoint Encryption Agents erstellt werden.

BEGRIFF	BESCHREIBUNG
Control Manager	Der Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops.
Domänenauthentifizierung	Die Authentifizierungsmethode, die Single Sign-On (SSO) mit Hilfe von Active Directory unterstützt.
DriveTrust™	Hardware-basierte Verschlüsselungstechnologie von Seagate™.
Encryption Management for Microsoft BitLocker	Der Endpoint Encryption Full Disk Encryption Agent für Microsoft Windows-Umgebungen, auf denen lediglich Microsoft BitLocker auf dem Hosting-Endpunkt aktiviert werden muss. Mit dem Encryption Management for Microsoft BitLocker Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Windows-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.
Encryption Management for Apple FileVault	Der Endpoint Encryption Full Disk Encryption Agent für Mac OS-Umgebungen, auf denen lediglich Apple FileVault auf dem Hosting-Endpunkt aktiviert werden muss. Mit der Encryption Management for Apple FileVault Agent können Sie Endpunkte mit Trend Micro Full Disk Encryption in einer bestehenden Mac OS-Infrastruktur sichern. Weitere Informationen finden Sie unter *Info über Full Disk Encryption auf Seite 14-2*.
Endpoint Encryption Gerät	Ein beliebiger Computer, ein Laptop oder ein Wechselmedium (externes Laufwerk, USB-Laufwerk), das von Endpoint Encryption verwaltet wird.

Begriff	Beschreibung
Endpoint Encryption Dienst	Der PolicyServer Dienst, der die gesamte Kommunikation mit Endpoint Encryption 5.0 Patch 1 Agents sicher verwaltet. Weitere Informationen finden Sie unter *Info über PolicyServer auf Seite 1-13*. Angaben zur Kommunikation von Endpoint Encryption 3.1.3 Agents und niedriger finden Sie unter Legacy Web Service.
Unternehmen	"Endpoint Encryption - Unternehmen" ist der eindeutige Bezeichner für das Unternehmen in der PolicyServer Datenbank, der bei der Installation von PolicyServer konfiguriert wurde. Eine PolicyServer Datenbank darf mehrere Unternehmenskonfigurationen haben. Jedoch darf es in Endpoint Encryption Konfigurationen mit Control Manager nur ein Unternehmen geben.
File Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien. Mit File Encryption können Sie die Dateien und Ordner auf nahezu jedem Gerät, das als Laufwerk im Host-Betriebssystem angezeigt wird, schützen. Weitere Informationen finden Sie unter *Info über die File Encryption auf Seite 13-2*.
FIPS	Federal Information Processing Standard. Der von der US-Regierung definierte Standard für Computersicherheit.
Festes Kennwort	Die Authentifizierungsmethode zur Verwendung herkömmlicher Benutzerkennwörter, die aus Buchstaben und/oder Ziffern und/oder Sonderzeichen bestehen.
Full Disk Encryption	Der Endpoint Encryption Agent für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung.

Begriff	Beschreibung
KeyArmor	Das mit Endpoint Encryption kennwortgeschützte und verschlüsselte USB-Laufwerk. **Hinweis** Endpoint Encryption 5.0 verfügt über keine KeyArmor Geräte. Es werden jedoch ältere KeyArmor Geräte unterstützt.
Legacy Web-Service	Der PolicyServer Dienst, der die gesamte Kommunikation mit Agents für Endpoint Encryption 3.1.3 und niedriger sicher verwaltet. Weitere Informationen finden Sie unter *Info über PolicyServer auf Seite 1-13*. Informationen zur Kommunikation mit Endpoint Encryption 5.0 Patch 1 finden Sie unter Endpoint Encryption Dienst.
OCSP	Online Certificate Status Protocol. Das Protokoll, das für digitale X.509- Zertifikate verwendet wird.
OfficeScan	OfficeScan schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus einem Agent am Endpunkt sowie einem Serverprogramm, das alle Agents verwaltet.
OPAL	Die Subsystemklasse für Sicherheit der Trusted Computing Group für Client-Geräte.
Kennwort	Alle Arten von Authentifizierungsdaten, die in Kombination mit einem Benutzernamen verwendet werden, wie feste Kennwörter, PINs und ColorCode.
PIN	Die Authentifizierungsmethode zur Verwendung einer PIN, die von Geldautomaten her bekannt ist.
PolicyServer	Der zentrale Verwaltungsserver, der die Richtlinien zur Verschlüsselung und Authentifizierung auf die Endpoint Encryption Agents verteilt.

Begriff	Beschreibung
Remote-Hilfe	Die Authentifizierungsmethode, um Endpoint Encryption Benutzer, die ihre Anmeldedaten vergessen haben, oder Endpoint Encryption Geräte, auf denen die Richtlinien nicht innerhalb eines festgelegten Zeitraums synchronisiert wurden, zu unterstützen.
Wiederherstellungskonsole	Die Benutzeroberfläche von Full Disk Encryption zur Wiederherstellung von Endpoint Encryption Geräten, wenn es zu einem Ausfall des primären Betriebssystems gekommen ist, Netzwerkprobleme untersucht werden und Benutzer, Richtlinien und Protokolle verwaltet werden.
Reparatur-CD	Die bootfähige CD von Full Disk Encryption, mit der ein Laufwerk entschlüsselt werden kann, bevor Full Disk Encryption entfernt wird, für den Fall, dass der Datenträger beschädigt wird.
RESTful	Representational State Transfer (Web-API). Das verschlüsselte AES-GCM-Kommunikationsprotokoll, das von Endpoint Encryption 5.0 Agents verwendet wird. Nachdem sich ein Benutzer authentifiziert hat, generiert PolicyServer ein Token im Zusammenhang mit der spezifischen Richtlinienkonfiguration. Ohne Authentifizierung verweigert der Dienst alle Richtlinientransaktionen. **Hinweis** Informationen zu AES-GCM finden Sie unter: http://tools.ietf.org/html/rfc5084#ref-GCM%3F
RSA SecurID	Ein Mechanismus zum Ausführen der Zwei-Faktor-Authentifizierung für einen Benutzer bei einer Netzwerkressource.
SED	Secure Encrypted Device (sicher verschlüsseltes Gerät). Eine Festplatte oder ein anderes Gerät, das verschlüsselt wurde.
Selbsthilfe	Die Authentifizierungsmethode, um Endpoint Encryption Benutzer dabei zu unterstützen, Antworten auf Sicherheitsfragen zu geben, bevor der Technische Support bei einem vergessenen Kennwort kontaktiert wird.

BEGRIFF	BESCHREIBUNG
Smartcard	Die Authentifizierungsmethode, bei der eine physische Karte zusammen mit einer PIN oder einem festen Kennwort erforderlich ist.
SOAP	Simple Object Access Protocol. Das verschlüsselte Kommunikationsprotokoll, das von allen Agents von Endpoint Encryption 3.1.3 (und älter) zur Kommunikation mit PolicyServer verwendet wird. In bestimmten Situationen erlaubt SOAP möglicherweise unsichere Richtlinientransaktionen ohne Benutzerauthentifizierung. Legacy Web Service filtert SOAP-Aufrufe, indem eine Authentifizierung erforderlich gemacht wird und die Befehle begrenzt werden, die SOAP akzeptiert.

Stichwortverzeichnis

A

Abfrageprotokolle, A-72
Active Directory, 1-10, 2-10, 2-11, 6-11, 11-20
    Benutzer importieren, 6-7, 11-6
    Kennwort zurücksetzen, 6-15, 11-24
Agent-Hierarchie, E-5, E-6
    Info über, E-5
    Spezifische Aufgaben, E-6
Agents, 1-18
    Dienste, E-13
ändern
    Registerkarten, 4-4
Angegebene Richtlinien, 5-4
    Priorität, 5-4
Anhänge, 1
anzeigen
    Protokolle für verwaltete Produkte, A-28
Ausstehende Ziele, 5-9
Authentifizierung, 1-2
    ColorCode, 2-7, 2-9, 13-6, 14-11
    Domäne, 2-10
    Domänenauthentifizierung, 2-7
    Festes Kennwort, 2-7, 2-12
    File Encryption, 13-2
    Full Disk Encryption, 14-3
    Info über, 2-1
    Kennwort ändern, 13-7
    Kontentypen, 2-6
    LDAP, 2-11
    Methode ändern, 14-8
    Optionen, 2-8
    PIN, 2-7, 2-12, 13-6
    Remote-Hilfe, 2-7, 2-12, 11-32, 14-13
    Selbsthilfe, 2-7, 2-14, 11-28, 14-16, 14-18
        Antworten, 14-18
    Setup-Voraussetzungen, 2-11
    Sicherheitsoptionen, 2-2, 13-9
    Single Sign-On, 13-3
    Smartcard, 2-15, 11-24, 11-25, 13-4, 14-14
    Voraussetzungen, 2-11
Authentifizierungsmethode, 2-7
Automatische Verteilungseinstellungen
    Zeitgesteuerter Download, A-63

B

Begriffe, F-1
Benutzer, 2-5, 6-1, 8-6, 11-1
    Active Directory-Kennwörter, 11-24
    ändern, 11-9
    Aus Gruppe entfernen, 10-12, 11-19
    Benutzer aus Richtlinie entfernen, 6-25
    Gelöschtes wiederherstellen, 6-27, 11-19, 16-11
    Gruppenmitgliedschaft, 11-10
    Gruppen- und Unternehmensänderungen, 11-9
    hinzufügen, 6-4, 11-3
    In eine Gruppe installieren, 11-17
    In Richtlinie installieren, 6-20
    Kennwörter, 6-11, 11-20
    Mit CSV importieren, 11-6
    Neuen Benutzer zur Gruppe hinzufügen, 8-9, 10-7, 11-11
    Neuen Unternehmensbenutzer hinzufügen, 8-12, 11-3
    Richtlinienmitgliedschaft, 6-17
    Sperrung, 3-26, 5-24

Standardgruppe ändern, 11-16
Standardrichtlinie ändern, 6-21
Suchen, 11-8
Von AD importieren, 6-7, 11-6
Vorhandenen Benutzer zur Gruppe hinzufügen, 8-15, 10-10, 11-14
Vorhandenen Benutzer zur Richtlinie hinzufügen, 6-22
Benutzer importieren, 11-6
Benutzer und Gruppen, 8-6
Berechtigungen anzeigen, 5-27
Berichte, 1-2, 16-1, 16-17
Alarm, 16-21, 16-22
Anzeigen von Berichten, 16-23
Einzelberichte, A-89
Fehler anzeigen, 16-24
Optionen, 16-18
Standard, 16-20, 16-21
Symbole, 16-19
Typen, 16-19
Vorlagen, A-74
zeitgesteuerte Berichte, 16-23, A-96
Berichtvorlagen, A-74
Bildschirmtastatur, 14-8
Boot wiederherst., 14-27

C

Client-Server-Architektur, 1-10
ColorCode, 2-9, 14-11
Command Line Helper, 14-2, 14-45, 14-46
Command Line Helper Installationsprogramm, 14-2
Community, 17-6
Control Manager, 1-17, 3-2, 3-5, A-1, A-6
Agent, 3-6, A-7
Benutzer
Aus Richtlinie entfernen, 6-25
Zur Richtlinie hinzufügen, 6-22
Berichtserver, 3-5, A-6
Funktionen, A-3
grundlegende Funktionen, A-3
Info über, 1-17, 3-2, A-1
Komponenten für Antivirenschutz und Content-Sicherheit, A-42, A-43
Konten, A-9
Konten konfigurieren, A-9
Mail-Server, 3-5, A-6
MCP, 3-6, A-7
Richtlinien, 5-1
SQL-Datenbank, 3-5, A-6
Trend Micro Management Infrastructure, 3-6, A-7
Verwaltetes Produkt, A-17
Webbasierte Management-Konsole, 3-7, A-8
Webserver, 3-5, A-6
Widget-Framework, 3-7, A-8
Control Manager Komponenten für Antivirenschutz und Content-Sicherheit
Anti-Spam-Regeln, A-42
Engines, A-42
Pattern-Dateien/Cleanup-Templates, A-42
CSV, 11-6

D

DAAutoLogin, 14-2, 14-45, 14-46
dashboard
verwenden, 4-2
Datenansichten
Grundlegendes, A-73
Datenschutz, 1-2
Datenwiederherstellung, 14-39
Deinstallieren

Agents, E-19
Demilitarisierte Zone, 14-19
Directory Manager, A-35
Discs brennen, 13-21
Domänenauthentifizierung, 2-10, 13-4
File Encryption, 13-3
Download Center, 17-5

E

Einstellungen für zeitgesteuerte Downloads
Einstellungen konfigurieren, A-62
Einstellungsberechtigungen, 5-27
Einstellungsberechtigungen ändern, 5-27
Encryption Management for Apple FileVault
Info über, 15-11
Encryption Management for Microsoft BitLocker
Agent-Dienst, E-13
Info über, 15-5
Endpunktverschlüsselung
Info über, 1-2
Tools, 14-2
Entschlüsselung
Wiederherstellungskonsole, 14-25
Entwurfsrichtlinien, 5-5
erstellen
Ordner, A-38

F

Fehlermeldungen
Authentifizierung, 2-2, 13-9
Festes Kennwort, 2-12
Festpl. entschlüss., 14-25
File Encryption, 13-1
Agent-Dienst, E-13
archivieren, 13-16
Archivieren und brennen, 13-16, 13-21
Archiv mit festen Kennwort brennen, 13-21
Archiv mit Zertifikat brennen, 13-21
Authentifizierung, 13-2
ColorCode, 13-6
Domäne, 13-3
Erstmals, 13-2
PIN, 13-6
Smartcard, 13-4
digitales Zertifikat, 13-20
erstellen, 13-20
Erste Verwendung, 13-2
fester Kennwortschlüssel
erstellen, 13-19
File Encryption, 13-2
Gemeinsamer Schlüssel, 13-17
erstellen, 13-18
Gerät entsperren, 11-33, 13-8
Kennwort ändern, 13-7
Kennwort zurücksetzen, 13-7, 13-11
lokaler Schlüssel, 13-16, 13-17
Mit PolicyServer synchronisieren, 13-12
Offline-Dateien synchronisieren, 13-13
PolicyServer Synchronisierung, 13-11
PolicyServer wechseln, 13-14
Remote-Hilfe, 11-33, 13-8
Sicheres Löschen, 13-22
Single Sign-On, 13-3
Smartcards, 13-5
Task-Leistensymbol
Info über, 13-11
Verschlüsselung, 13-16
FIPS
FIPS 140-2, 1-9
Info über, 1-9

Sicherheitsstufen, 1-9
Full Disk Encryption, 14-1
Agent-Dienst, E-13
Authentifizierung, 2-14, 14-16
Kennwort ändern, 14-10
Dateien entfernen, 14-44
Deinstallieren, 14-34
Festpl. entschlüss., 14-25
Konnektivität, 14-19
Menüoptionen, 14-4
Netzwerkkonfiguration, 14-31
Netzwerk-Setup, 14-31
patching, 14-47
PolicyServer Einstellungen, 14-19
PolicyServer wechseln, 14-24
Porteinstellungen, 14-19
Remote-Hilfe, 11-32, 14-13
Selbsthilfe, 14-17
Synchronisierung von Richtlinien, 14-20
TCP/IP-Zugriff, 14-19
Tools, 14-2
Unternehmen wechseln, 14-32
wechseln, 14-24, 14-34
Wiederherstellungskonsole, 14-23
Benutzer verwalten, 14-28
Richtlinien verwalten, 14-31
Windows, 14-24
Wiederherstellungsmethoden, 14-34
Windows patches, 14-45
Full Disk Encryption Preboot, 14-3
Authentifizierung, 14-8
Bildschirmtastatur, 14-8
Menüoptionen, 14-4
Netzwerkverbindung, 14-5
Tastaturbelegung, 14-8
Wireless-Verbindung, 14-5
Funktionen, A-3

G

Gefilterte Richtlinien, 5-5
Neuordnen, 5-5
Gerät, 1-2
Geräte, 2-2, 4-12, 7-1, 7-7, 12-1
Attribute anzeigen, 7-12, 12-8
Aus Gruppe entfernen, 10-14, 12-4
Aus Richtlinie entfernen, 7-6
Befehl "Auslöschen", 2-5, 7-15, 12-13
Entfernen, 7-17, 12-5
Gruppenmitgliedschaft, 12-12
neu starten, 2-5, 7-17, 12-14
Software-Token, 2-4, 7-10, 12-6
Sperren, 2-5, 3-26, 5-24, 7-16, 12-14
Suchen, 7-9
Unternehmensgerät entfernen, 7-17, 12-5
Verzeichnisliste, 12-12
Wiederherstellungsschlüssel, 2-4, 7-11, 12-7
Zur Gruppe hinzufügen, 10-13, 12-3
Zur Richtlinie hinzufügen, 7-3
Grundlegendes
Datenansichten, A-73
Protokollabfragen, A-72
Protokolle, A-70
Verteilungspläne, A-65
Gruppen, 8-6, 10-1
ändern, 10-6
entfernen, 10-6
Gerät entfernen, 10-14, 12-4
In eine Gruppe installieren, 11-17
Offline-Gruppen, 10-15
Offline-Gruppen erstellen, 10-15
Typen, 10-2
Untergruppen, 10-2

H

Häufigkeit des zeitgesteuerten Downloads
    Konfigurieren, A-61
Helpdesk-Richtlinien, 11-31

I

Info über
    Authentifizierung, 2-1
    Benutzer, 8-6
    Client-Server-Architektur, 1-10
    Encryption Management for Apple FileVault, 15-11
    Encryption Management for Microsoft BitLocker, 15-5
    Endpoint Encryption Dienst, 1-13
    Endpunktverschlüsselung, 1-2
    File Encryption, 13-1, 13-2
    FIPS, 1-9
    Full Disk Encryption
        Encryption Management for Apple FileVault, 14-2
        Encryption Management for Microsoft BitLocker, 14-2
    Gruppen, 8-6
    Integration des Control Managers, 3-2
    Kontentypen, 2-6
    Legacy Web-Service, 1-13
    OfficeScan, E-2
    PolicyServer, 1-13, 3-1, 8-1
    PolicyServer MMC, 8-2
    Wartungsvertrag, 17-2
    Widgets, 4-5

K

Kennwörter, 1-2, 6-11, 11-20
    Active Directory zurücksetzen, 6-15
    Auf ein festes Kennwort zurücksetzen, 11-23
    Benutzer zurücksetzen, 6-14, 6-15
    Festes Kennwort ändern, 6-16
    Festes Kennwort zurücksetzen, 6-14
    Methode ändern, 6-16
    Remote-Hilfe, 11-29
    Richtlinienadministrator/ Authentifizierer zurücksetzen, 6-13
    Selbsthilfe, 11-28
    Unternehmensadministrator/ Authentifizierer zurücksetzen, 6-12
    Zurücksetzen, 6-12, 6-13, 11-22
        Active Directory, 11-24
        Benutzer, 11-23, 11-24
        Gruppenadministrator, 11-22
        Gruppenauthentifizierer, 11-22
        Unternehmensadministrator, 11-21
        Unternehmensauthentifizierer, 11-21
Kennwörter ändern, 14-10
Komponenten
    herunterladen, A-41
Komponenten herunterladen
    manuell, A-44
Komponenten herunterladen und verteilen, A-41
Konfigurieren, A-61
    Benutzerkonten, A-9
    Einstellungen für zeitgesteuerte Downloads, A-62
    Verwaltete Produkte, A-26
    Zeitgesteuerte Download-Ausnahmen, A-51
    Zeitgesteuerter Download

Automatische Verteilungseinstellungen, A-63
Konten
Typen, 2-6

L

LDAP, 2-11
LDAP-Proxy, 6-4, 11-3
Liste der verwalteten Server, 5-31
Proxy-Einstellungen konfigurieren, 5-35
Server bearbeiten, 5-35
löschen
Registerkarten, 4-4

M

Manuelles Herunterladen von Komponenten, A-44
MBR
Ersetzen, 14-27
MCP, 3-6, A-7

N

Netzwerk-Setup, 14-31

O

OfficeScan
Agents deinstallieren, E-19
Online
Community, 17-6
Optionen der Verzeichnisverwaltung, A-37
Ordner
erstellen, A-38
umbenennen, A-39

P

Persönliche Identifikationsnummer (PIN), 2-12
Plug-in-Manager, E-3
PolicyServer
Anwendungen aktivieren, 8-21
Benutzeroberfläche, 8-4
Berichte, 16-1, 16-17
Client-Web-Service, 1-10
Erste Schritte, 3-1, 8-1
Erweiterter Standort, 16-17
MMC-Fenster, 9-4
MMC-Hierarchie, 8-5
Protokolle, 16-1
Protokollereignisse, 16-12
Protokollwarnungen einrichten, 16-14
Remote-Hilfe, 11-29
Richtlinien, 5-7, 9-1, 9-2, 9-4
Bearbeiten, 9-4
Support-Informationen, 11-31
Smartcard, 11-25
SMS/E-Mail-Versand weiterleiten, 16-15
Support-Informationen, 11-31
Untergruppen, 10-5
Verbesserungen, 1-4
Wartung, 16-2
PolicyServer MMC, 1-10
Authentifizierung, 8-2
Benutzer, 8-6
Unternehmensbenutzer hinzufügen, 8-9, 10-7, 11-11
Zur Gruppe hinzufügen, 8-9, 8-15, 10-7, 10-10, 11-11, 11-14
Benutzer und Gruppen, 8-6
Erstverwendung, 8-2
Felder und Schaltflächen, 8-17, 9-3
Gruppen, 8-6
Benutzer hinzufügen, 8-9, 10-7, 11-11
Offline-Gruppen, 10-15

Aktualisieren, 10-18
erstellen, 10-15
Richtlinien, 8-16
Bearbeiten
Mehrere Optionen, 9-13
Mehrfachauswahl, 9-9
Richtlinien mit Bereichen, 9-5
Textzeichenfolge, 9-12
Wahr/Falsch, Ja/Nein, 9-7
Richtlinien ändern, 8-18
Top-Gruppe hinzufügen, 8-7, 10-3
Unternehmensbenutzer hinzufügen, 8-12, 11-3
Produktdefinitionen, F-1
Produktkomponenten, 1-10
Produktübersicht, 1
Produktverzeichnis
Komponenten verteilen, A-24
Protokolle, 14-31, 16-1, A-70
Abfragen, A-72
Ereignisse verwalten, 16-13
Warnungen, 16-14
Warnungen einrichten, 16-14
Protokollereignisse, 16-12
Proxy-Einstellungen
Liste der verwalteten Server, 5-35
Proxy-Einstellungen konfigurieren
Liste der verwalteten Server, 5-35

R

Registerkarten
ändern, 4-4
Info über, 4-2
löschen, 4-4
Übersichtsdashboard, 4-2
Registrieren
bei Control Manager, A-8
Registrierung
Profil, 17-2
Schlüssel, 17-2
URL, 17-2
Remote-Hilfe, 2-2, 2-5, 2-12, 6-11, 7-16, 11-20, 11-29, 12-14, 13-9, 14-13
Reparatur-CD, 14-2, 14-34, 14-37
Datenwiederherstellung, 14-39
Entschlüsselung, 14-40
Richtlinie
Geräte installieren, 6-20
Richtlinie "Anmelden als Stapelverarbeitungsauftrag", A-69
Richtlinien, 1-2, 5-14
Allgemein, 3-23, 5-21, 9-33
Agent, 9-34
Authentifizierung, 9-34
Bearbeiten, 5-29, 6-22, 6-25
Benutzer, 3-16, 5-14
File Encryption, 3-20, 5-18
Anmelden, 9-31
Computer, 9-28
Kennwort, 9-33
Verschlüsselung, 9-29
Full Disk Encryption, 3-18, 5-16, 9-21, 9-28, 14-20
Anmelden, 9-22
Client, 9-21
Kennwort, 9-27
Verschlüsselung, 9-22
Gerät entfernen, 7-6
Indikatoren, 8-17, 9-2
löschen, 5-30
PolicyServer, 9-16
Administrator, 9-16
Authentifizierer, 9-18

Begrüßungsnachricht, 9-20
Herunterladen von Service Packs, 9-19
Konsole, 9-16
Protokollwarnungen, 9-19
Richtlinienzuordnung, D-1
Support-Informationen, 11-31
Synchronisieren, 14-20
Synchronisierung, 14-2
Wiederherstellung durch Benutzer zulassen, 14-23
Richtlinien bearbeiten, 5-29, 6-22, 6-25
Richtlinieneinstellungen
Kopieren, 5-28
Richtlinieneinstellungen kopieren, 5-28
Richtlinien erstellen
Einstellungen kopieren, 5-28
Einstellungsberechtigungen, 5-27
Zentrale Verwaltung, 5-28
Richtlinienliste, 5-5, 5-8
Richtlinien löschen, 5-30
Richtlinienpriorität, 5-8
Richtliniensteuerung, 13-1
Richtlinientypen
Angebe, 5-4
Entwurf, 5-5
Gefiltert, 5-5
Richtlinienpriorität, 5-8
Richtlinienverwaltung, 5-2
Angegebene Richtlinien, 5-4
Ausstehende Ziele, 5-9
Einstellungsberechtigungen, 5-27
Entwurfsrichtlinien, 5-5
Gefilterte Richtlinien, 5-5
Liste der verwalteten Server, 5-31
Richtlinien bearbeiten, 5-29, 6-22, 6-25
Richtlinieneinstellungen kopieren, 5-28
Richtlinienliste, 5-5, 5-8
Richtlinien löschen, 5-30
Richtlinien neu ordnen, 5-5
Richtlinienpriorität, 5-4, 5-8
Richtlinienvorlagen aktualisieren, 5-36
verstehen, 5-2
Verwaltete Server bearbeiten, 5-35
Zentrale Verwaltung, 5-28
Ziele, 5-9
Richtlinienvorlagen, 5-36
Richtlinienvorlagen aktualisieren, 5-36
Richtlinienziele, 5-9
Richtlinienzuordnung
Control Manager, D-1
PolicyServer, D-1

S

Selbsthilfe, 2-14, 6-11, 11-20, 14-16
Antworten, 14-18
Antworten festlegen, 14-17
Kennwortunterstützung, 11-28
Sicherheit
Antivirus-/Anti-Malware-Schutz, 1-2
Gerätesperre, 2-12, 14-13
Gerät löschen, 2-2, 13-9
Kontosperraktion, 2-12, 14-13
Kontosperre, 2-12, 14-13
Remote-Authentifizierung erforderlich, 2-2, 13-9
Zeitraum bis Kontosperrung, 2-12, 14-13
Zeitverzögerung, 2-2, 13-9
Zulässige Anzahl fehlgeschlagener Anmeldeversuche, 2-12, 14-13
Smartcard, 2-15, 11-24, 14-14
Authentifizierung, 11-25
Smartcards, 2-15, 11-24, 14-14

SSO, 2-10
Suchen
    Verwaltete Produkte, A-34
Support
    Knowledge Base, 17-6
    Schnellere Problemlösung, 17-8
    TrendLabs, 17-10
Synchronisierung
    File Encryption, 13-12

T

Testlizenz, 17-3
Token, 11-25, 11-27, 14-16
Tools
    Command Line Helper, 14-45
    DAAutoLogin, 14-45
    Reparatur-CD, 14-37
    Wiederherstellungskonsole, 14-32
Top-Gruppe, 8-7, 10-3
TrendLabs, 17-10
Trend Micro Control Manager
    Benutzerzugriff auf verwaltete Produkte, A-11
    Registrieren bei, A-8

U

Übersichtsdashboard, 4-1
    Hinzufügen von Registerkarten, 4-3
    Registerkarten, 4-2
    Registerkarten ändern, 4-4
    Registerkarten löschen, 4-4
umbenennen
    Ordner, A-39
    Verwaltete Produkte, A-39
URL
    Registrierung, 17-2

V

Verschlüsselung, 1-9, 9-29
    Archivieren, 13-21
    Datei und Ordner, 13-2
    digitales Zertifikat, 13-20
    fester Kennwortschlüssel, 13-18
    File Encryption, 13-1
        Archivieren und brennen, 13-16
    FIPS, 1-9
    Funktionen, 1-2
    Hardware-basiert, 1-9, 14-2
    lokaler Schlüssel, 13-16
    Schlüssel
        gemeinsame, 13-17
    selbstextrahierend, 13-18
    Software-basiert, 1-9, 14-2
    Vollständige Festplatte, 14-2
verstehen
    Endpunktverschlüsselung, 1-1
Verteilung
    OfficeScan, E-10–E-12
Verteilungspläne, A-65
Verwaltete Produkte
    Aufgaben erteilen, A-27
    Konfigurieren, A-26
    Protokolle anzeigen, A-28
    suchen, A-34
    umbenennen, A-39
    Wiederherstellen, A-32
Verwaltete Server bearbeiten, 5-35

W

Warnungen, 16-14
Wartung, 16-2
Wartungsvertrag
    Ablauf, 17-2
    Info über, 17-2

Verlängerung, 17-2
Wichtigste Funktionen, 1-2
Widgets
Anpassen, 4-7
Beschreibung, 4-9
Endpoint Encryption - Bericht zu Sicherheitsverstößen, 4-25
Endpoint Encryption - Gerätesperrung, 4-23
Endpoint Encryption Status, 4-15
Endpunktverschlüsselung, 4-9
Erfolglose Anmeldeversuche am Endpoint Encryption Gerät, 4-18
Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers, 4-20
hinzufügen, 4-6
Hinzufügen von Registerkarten, 4-3
Konfigurieren, 4-8
löschen, 4-9
Optionen, 4-8
verstehen, 4-5
Wiederherstellen
Verwaltete Produkte, A-32
Wiederherstellung
Dateien entfernen, 14-44
Wiederherstellungskonsole, 14-21
Anmelden, 14-23
Anmeldung, 14-24
Benutzer
Bearbeiten, 14-29
Hinzufügen, 14-30
Löschen, 14-30
Benutzer verwalten, 14-28
Boot wiederherst., 14-27
Festpl. entschlüss., 14-25
Funktionen, 14-21
Netzwerkkonfiguration, 14-31
Netzwerk-Setup, 14-31
Partit. bereitst., 14-27
PolicyServer wechseln, 14-24, 14-34
Protokolle anzeigen, 14-31
Reparatur-CD, 14-40
Richtlinien verwalten, 14-31
Unternehmen wechseln, 14-32
Wiederherstellungsmethoden, 14-34
Zugreifen, 14-23
Windows, 14-24
Wiederherstellungsmethoden, 14-34
Windows Patch-Verwaltung, 14-45

Z

Zeitgesteuerte Download-Ausnahmen
Konfigurieren, A-51
Zeitgesteuerte Downloads, A-53
Zeitgesteuerter Download
Konfigurieren
Automatische Verteilungseinstellungen, A-63
Zeitplan für zeitgesteuerte Downloads
Konfigurieren, A-61
Zeitplanleiste, A-13
Zeitplan und Häufigkeit für zeitgesteuerte Downloads, A-61
Zentrale Verwaltung, 1-2, 5-28
Ziele, 5-9
Ausstehend, 5-9
Zugänglichkeit
Bildschirmtastatur, 14-8

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799 info@trendmicro.com

www.trendmicro.de

Item Code: APGM56401/140410